AML/CFT – TERMINOLOGICKÁ PRÍRUČKA PRE PRAX

ZÁKLADNÝ SLOVNÍK POJMOV

G. Lehnert
LAWYERS WITH INTEGRITY

G. Lehnert, s. r. o.
Budova ORBIS, Rajská 7, SK-811 08 Bratislava
lehnert@lehnert.sk | www.lehnert.sk

PRÍHOVOR

Oblasť boja proti praniu špinavých peňazí a financovaniu terorizmu – skrátene AML/CFT – patrí k témam, ktoré sa na prvý pohľad môžu zdať vzdialené každodennému životu. Opak je pravdou. Dotýkajú sa každej finančnej transakcie, každého obchodného vzťahu, každej inštitúcie, ktorá narába s peniazmi – a v konečnom dôsledku nás všetkých. Najmä sa však týka všetkých tzv. povinných osôb v zmysle zákona č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu, v znení neskorších predpisov.

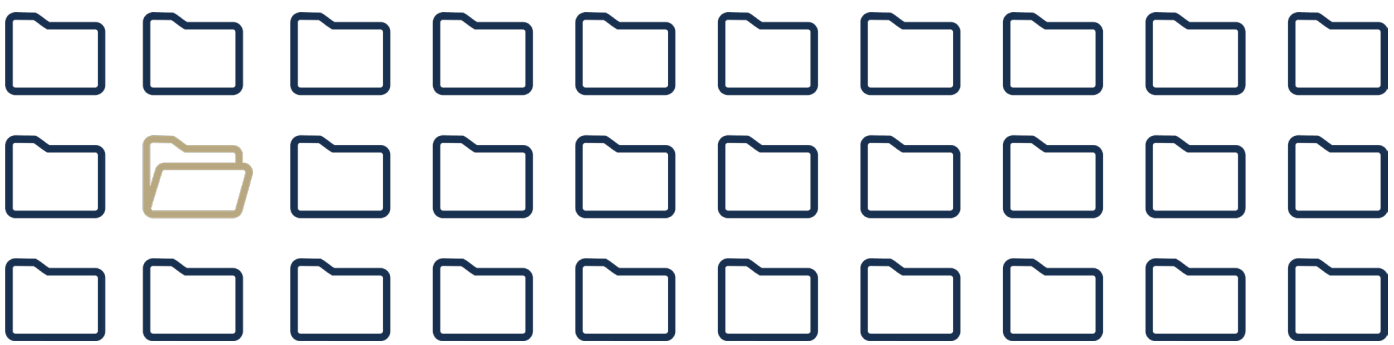
Táto problematika je rozsiahla, globálna a neustále sa vyvíjajúca. Regulačný rámec sa buduje na desaťročiach medzinárodnej spolupráce, stovkách právnych predpisov, odporúčaní a usmernení vydávaných orgánmi po celom svete. Nie je jednoduché sa v ňom orientovať – a to ani pre odborníkov, ktorí sa mu venujú každý deň.

Jednou z najväčších výziev pritom nie je nedostatok informácií, ale ich správne pochopenie. V praxi sa opakovane stretávame s tým, že pojmy z oblasti AML/CFT sú síce bežne používané, no ich skutočný obsah a presný rozsah zostávajú nejasné. Hranica medzi tým, čo si myslíme, že vieme, a tým, čo skutočne vieme, je v tejto oblasti prekvapivo tenká.

Práve z tohto dôvodu sme sa v G. Lehnert rozhodli pristúpiť k zostaveniu tohto glosára. Nie s ambíciou nahradiť odbornú literatúru či právne poradenstvo – ale s úprimnou snahou poskytnúť každému, kto sa s problematikou AML/CFT stretáva, spoľahlivý a zrozumiteľný základ. Základňu, od ktorej sa možno odraziť. Slovník, ktorý odpovedá skôr, než vznikne potreba dlhého hľadania.

Veríme, že tento príspevok bude užitočný – či už pre klientov, ktorí sa s regulačnými požiadavkami stretávajú prvýkrát, alebo pre tých, ktorí si chcú systematicky utriediť to, čo už vedia. Ak táto príručka pomôže čo i len trochu sprehľadniť komplexný svet AML/CFT, splnila svoj účel.

G. Lehnert



A

Account ... 6
Alert ... 6
Alternative Remittance System (ARS) ... 6
AMLA (Anti-Money Laundering Authority) ... 6
Anti-Money Laundering Directive (AMLD) ... 6
Anti-Money Laundering International Database (AMLID) ... 6
Anti-Money Laundering Program ... 7
Arrest Warrant ... 7
Asia/Pacific Group on Money Laundering (APG) ... 7
Asset ... 7
Asset Blocking (Blokovanie majetku) ... 7
Asset Confiscation ... 8
Asset Flight ... 8
Asset Forfeiture (Prepadnutie majetku) ... 8
Asset Freezing ... 8
Asset Mingling ... 8
Asset Protection ... 9
Asset Protection Trusts (APTs) ... 9
Asset Recovery ... 9
Asset Tracing ... 9
Automated Clearing House (ACH) ... 9
Automated Screening Tool (AST) ... 9
Automated Teller Machine (ATM) ... 9

B

Back-to-Back Letters of Credit ... 10
Bank Draft ... 10
Bank Secrecy ... 10
Bank Secrecy Act (BSA) ... 10
Bank Secrecy Act Compliance Program ... 10
Basel Committee on Banking Supervision (Basel Committee) ... 10
Batch Transfer ... 10
Batch Processing ... 10
Batch Screening ... 11
Bearer Form (Forma na doručiteľa) ... 11
Bearer Negotiable Instruments (BNIs) ... 11
Bearer Share ... 11
Benami Account ... 11
Beneficial Owner ... 11
Beneficial Ownership Register ... 12
Beneficiary ... 12
Beneficiary Financial Institution ... 12
Bill of Exchange (Zmenka) ... 12
Bill of Lading (Nákladný List) ... 12
Bill Stuffing ... 12
Blacklist ... 12
Black Market Peso Exchange (BMPE) ... 12
Blockade ... 13
Boycott ... 13
Bureau of Industry and Security (BIS) ... 13

C

Cardholder ... 13
Caribbean Financial Action Task Force (CFATF) ... 13
Casa de Cambio (Zmenáreň) ... 13
Cash-Intensive Business ... 13
Cash Collateralized Loans ... 13
Cash Deposits ... 13
Cashier's Check ... 14
Central Bank Digital Currency (CBDC) ... 14
Comisión Interamericana para el Control del Abuso de Drogas or Inter-American Drug Abuse Control Commission (CICAD) ... 14
Collection Accounts ... 14
Commission Rogatoire ... 14
Competent Authorities ... 14
Compliance ... 14
Concentration Account ... 15
Concentration Risk ... 15
Confidentiality ... 15
Confiscation ... 15
Consolidation of Goods ... 15
Control Effectiveness ... 15
Core Principles (CPs) ... 16
Corporate Vehicles ... 16
Correspondent Banking ... 16
Counter Terrorist Action Group (CTAG) ... 16
Counter-Terrorism Financing (CTF/CFT) ... 16
Counter-Terrorism Committee (CTC) ... 16
Credit Card ... 16
Criminal Proceeds ... 16
Cross-Border ... 16
Currency ... 16
Currency Smuggling ... 17
Currency Transaction Report (CTR) ... 17
Custodian ... 17
Custody ... 17
Customer Due Diligence (CDD) ... 17
Customer Relationship ... 17
Customer Risk Rating / Risk Scoring ... 17

D

De-Risking ... 17
Dealing in Funds ... 17
Debit Card ... 17
Decision Tree ... 17
Delisting ... 18
Delivery Channel ... 18
Denied Persons List (DPL) ... 18
Designated Categories of Offense ... 18
Designated Non-Financial Businesses and Professions ... 18
Designated Person or Entity ... 18
Designation ... 19
Dilution of Sanctioned Ownership ... 19
Dollar Clearing ... 19
Domestic Transfer ... 19
Dual Control ... 19
Dual-Use Goods ... 19
Due Diligence ... 19

E

Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) ... 20
Economic Sanctions ... 20
Egmont Group of Financial Intelligence Units ... 20
Electronic Funds Transfer (EFT) ... 20
Electronic Money (E-Money) ... 20
Embargo ... 20
Embezzlement ... 20
End-User Certificate ... 20
Enforceable Means ... 21
Enhanced Due Diligence (EDD) ... 21
Euroasian Group on Combating Money Laundering and Financing of Terrorism (EAG) ... 21
Europol ... 21
Evasion ... 21
Event-Triggered Monitoring ... 21
Exclusion List ... 21
Ex Parte ... 21
Export Administration Regulations (EAR) ... 22
Export Control Joint Unit (ECJU) ... 22
Express Trust ... 22
External Evasion ... 22
Extradiction ... 22
Extraterritorial Jurisdiction (ETJ) ... 22
Extraterritorial Reach ... 22

F

Facilitation (Uľahčenie/Napomáhanie) ... 22
False Declaration ... 23
False Disclosure ... 23
False Negative ... 23
False Positive ... 23
Final Rule Part 504 ... 23
Financial Group ... 23
Financial Institution ... 23
Financial Action Task Force (FATF) ... 24
FATF Recommendations ... 24
Financial Action Task Force-Style Regional Body (FSRB) ... 24
Financial Intelligence Unit (FIU) ... 24
Financial Sector Assessment Programme (FSAP) ... 24
Financial Stability Board (FSB) ... 25
FinTech (Financial Technology) ... 25
First Line of Defense ... 25
Follow-Up Reports ... 25
Foreign Counterparts ... 25
Foreign Sanctions Evader (FSE) ... 25
Forfeiture ... 25
Free Trade Zone (FTZ) ... 25
Freeze ... 25
Front Company ... 25
Fundamental Principals of Domestic Law ... 26
Funds or Other Assets ... 26
Fuzzy Logic ... 26

G

Gatekeepers ... 26
Global Magnitsky Act ... 26
Global Programme Against Money Laundering (GPML) ... 26
Globalization ... 26
Governance ... 27
Grantor ... 27
Greylist ... 27
Gulf Cooperation Council (GCC) ... 27

H

Hawala ... 27
Hawalada/Hawaladar ... 27
Hit ... 27
Human Rights ... 27
Human Smuggling ... 27
Human Trafficking ... 27

I

Identifier ... 27
Identification Data ... 27
Identity Theft ... 28
Intergovernmental Action Group Against Money-Laundering in West Africa (GIABA) ... 28
Intermediary Financial Institution ... 28
International Money Laundering Information Network (IMOLIN) ... 28

International Monetary Fund (IMF) ... 28
International Organizations ... 28
Inequalities List ... 28
Inherent Risk ... 28
Integration ... 28
Internal Evasion ... 29
International Business Company (IBC) ... 29
Investigation ... 29
International Organisation of Securities Commissions (IOSCO) ... 29
Isolation Company ... 29

J

Joint Comprehensive Plan of Action (JCPOA) ... 29
Jurisdiction of Citizenship ... 29
Jurisdiction of Residence ... 29

K

Kleptocrat ... 29
Know Your Business (KYB) ... 29
Knowledge ... 30
Know Your Customer (KYC) ... 30
Know Your Employee (KYE) ... 30

L

Law ... 30
Layering (Vrstvenie) ... 30
Legal Arrangement ... 31
Legal Risk ... 31
Letter of Credit ... 31
License ... 31
Limited Liability Company (LLC) ... 31
Look-Back (or Look-Back Review) ... 31

M

Mandatory Sanctions Lists ... 31
Memorandum of Understanding (MOU) ... 31
Middle East and North Africa Financial Action Task Force (MENAFATF) ... 31
MiLTech (Military Technology) ... 31
Mirror Trade ... 31
Mixing/Tumbling ... 32
Monetary Instruments ... 32
Money Laundering ... 32
Money Laundering Reporting Officer (MLRO) ... 32
Money Order (Peňažná poukážka) ... 32
Money Services Business (MSB) ... 32
Money Transfer Service or Value Transfer Service ... 32
MONEYVAL ... 32
Monitoring ... 33
Multilateral Sanctions ... 33
Mutual Evaluations ... 33
Mutual Evaluation Report (MER) ... 33
Mutual Legal Assistance Treaty (MLAT) ... 33

N

Name Screening ... 33
Naming Conventions ... 33
National Risk Assessment (NRA) – Národné hodnotenie rizík ... 33
Nested Account ... 33
Nesting ... 33
NTF (Non-Fungible Token) ... 34
Nominee Director or Shareholder ... 34
Non-Conviction Based Confiscation ... 34
Non-Cooperative Countries & Territories (NCCT) ... 34
Non-Governmental Organization (NGO) ... 34
Non-Profit Organizations (NPO) ... 34
Non-Proliferation Treaty (NPT) ... 34

O

Office for Foreign Assets Control (OFAC) ... 34
Office of the Superintendent of Financial Intitutions (OSFI) ... 34
Offshore ... 35
Offshore Banking License ... 35
Offshore Finance ... 35
Offshore Financial Center (OFC) ... 35
Offshore Group of Banking Supervisors (OGBS), Group of International Finance Centre Supervisors ... 35
Ongoing Due Diligence ... 35
Operational Risk ... 35
Ordering Financial Institution ... 36
Organization for Economic Cooperation and Development (OECD) ... 36
Originator ... 36

P

Palermo Convention ... 36
Partial Match ... 36
Pass-Through Sanctions Risk ... 36
Payable Through Account ... 36
Payment Screening ... 36
Payments, Cross Border ... 37
Physical Cross-Border Transportation ... 37
Physical Presence ... 37
Placement ... 37
Politically Exposed Person (PEP) ... 37
Ponzi Scheme/Pyramid Scheme ... 37
Predicate Crimes ... 37
Prepaid Card ... 37
Private Banking ... 37
Private Investment Company (PIC) ... 38
Proceeds ... 38
Proliferation Financing (Financovanie šírenia zbraní hromadného ničenia) ... 38
Property ... 38

R

Real Time Gross Settlement Systems (RTGS) ... 38
Reasonable Approach ... 38
Reasonable Cause (to Suspect) ... 38
Red Flag ... 38
Register, Corporate ... 38
RegTech (Regulatory Technology) ... 39
Regulatory Agency ... 39
Relatives and Close Associates (RCA) ... 39
Remittance Services ... 39
Reporting Requirements, Initial and Periodic ... 39
Reputational Risk ... 39
Respondent Bank ... 39
Risk Appetite ... 39
Risk Assessment ... 39
Risk-Based Approach ... 39
Romanization ... 39

Q

Qualifying Wire Transfers ... 40

S

Sanction Screening ... 40
Satisfied ... 40
Safe Harbor ... 40
Sanctions ... 40
Sanctions Compliance ... 40
Sanctions Compliance Officer (SCO) ... 40
Sanctions Compliance Program (SCP) ... 40
Sanctions Evasion ... 40
Sanctions Due Diligence (SDD) ... 40
Sanctions List ... 40
Sanctions Regime ... 40
Scope of Licensing ... 40
Scope of Permitted Activities ... 40
Second Line of Defense ... 41
Secondary Sanctions ... 41
Sectoral Sanction ... 41
Sectoral Sanctions Identification List (SSI List) ... 41
Seize ... 41
Self-Regulatory Body (SRB) ... 41
Senior Foreign Political Figure ... 41
Serial Payment ... 41
Settlors ... 41
Sham Divestment ... 41
Shanghai Cooperation Organization (SCO) ... 41
Shelf Company ... 41
Shell Bank ... 41
Shell Company ... 41
Should ... 41
Simple Checks ... 41
Simplified Due Diligence (SDD) ... 42
Smurfing ... 42
Source of Funds/Source of Wealth ... 42
Sources, Primary ... 42
Sources, Secondary ... 42
Specially Designated Nationals and Blocked Persons List (SDN List) ... 42
Sting Operation ... 42
Straight-Through Processing ... 42
Straw Man ... 42
Strict Liability ... 42
String Matching ... 42
Stripping ... 42
Structuring ... 42
Supervisors ... 42
Subpoena ... 43
Suspicious Activity Report (SAR) ... 43
Suspicious Transaction Report (STR) ... 43
SWIFT Message ... 43

T

Target Match ... 43
Targeted Sanctions ... 43
Tax Haven ... 43
Terrorist ... 43
Terrorist Act ... 43
Terrorist Financing ... 43
Terrorist Financing Abuse ... 43
Terrorist Financing Convention ... 43
Terrorist Financing Offence ... 43
Terrorist Organization ... 43
Testimony ... 44
Third Line of Defense ... 44
Third Parties ... 44
Threshold Calibration ... 44
Tipping Off ... 44
Toll Gates ... 44

Trade-Based Money Laundering (TBML) 44
Transaction Monitoring and Filtering Programs (TMPs) 44
Transliteration 44
Transparency International (TI) 44
Transshipment 44
Trust 44
Trustee 44
Typology 44

U

Unilateral Sanctions 44
United Nations (UN) 45
United Nations General Assembly (UNGA) 45
United Nations Office on Drugs and Crime (UNODC) 45
United Nations Security Council (UNSC) 45
UN Security Council Resolution 1373 (2001) 45
Unique Transaction Reference Number 45
Unusual Transaction 45
USA Patriot Act 45
U-Turn Payment 45

V

Vienna Convention 45
Virtual Asset 45
Virtual Asset Service Providers (VASP/CASP) 45
Virtual Currency 46

W

Weak Alias 46
Whitelist 46
Willful Blindness 46
Wire Transfer 46
Without Delay 46
Wolfsberg Group 46
World Bank (WB) 46
WGEL 46
WGTA 46
WGTYP 46

Tento Glosár obsahuje stručné vysvetlenia niektorých vybraných pojmov spojených s problematikou AML/CFT. Vychádza zo zaužívanej terminológie, ako aj z definícii pojmov tak, ako sú obsiahnuté v odporúčaniach FATF a v iných relevantných dokumentoch. Vzhľadom na špecifiká oblasti AML/CFT je potrebné brať v úvahu, že slovenský právny poriadok môže s danou definíciou spájať iný obsah, ako je bežne v medzinárodnom kontexte štandardizovaný, z tohoto dôvodu boli v glosári ponechané zaužívané anglické výrazy, ktorých štandardizovaný obsah je následne stručne vysvetlený v samotnom popise v slovenskom jazyku.

ACCOUNT

Pojem „účet" označuje v bežnom jazyku zmluvný vzťah medzi klientom a finančnou inštitúciou, v rámci ktorého inštitúcia spravuje zverené prostriedky a eviduje transakcie. V kontexte AML/CFT má však tento pojem podstatne širší záber – zahŕňa akýkoľvek obchodný vzťah medzi finančnou inštitúciou a klientom umožňujúci pohyb alebo správu finančných prostriedkov, vrátane úverových vzťahov, záložných účtov, vzťahov v rámci korešpondenčného bankovníctva, účtov kolektívneho investovania či vzťahov so sprostredkovateľmi. Povinnosti v oblasti AML/CFT – identifikácia a overovanie klienta (KYC/CDD), monitorovanie transakcií a hlásenie podozrivých aktivít – sa vzťahujú na všetky tieto vzťahy rovnako, bez ohľadu na ich formálne pomenovanie.

ALERT

Preskúmanie na základe základných červených vlajok *(red flags),* ktoré si vyžadujú pozornosť analytika. V rámci postupov poznania zákazníka *(KYC)* sú tieto upozornenia/varovania chápané ako potenciálne nezrovnalosti, ktoré sa označujú buď manuálne, alebo prostredníctvom automatizovaného systému na základe definovaných červených príznakov a základných typológií. V rámci kontroly sankcií je upozornenie zhoda alebo viacnásobná zhoda interného záznamu. Ak sa nedajú jednoducho vyriešiť ako falošne pozitívne výsledky *(false positive),* varovania spravidla vedú k vyšetrovaniu.

ALTERNATIVE REMITTANCE SYSTEM (ARS)

„Podzemné" bankovníctvo alebo neformálne systémy prevodu hodnôt *(IVTS).* Často sa spája s etnickými skupinami z Blízkeho východu, Afriky alebo Ázie a bežne zahŕňa prevod hodnôt medzi krajinami mimo formálneho bankového systému. Subjektom vykonávajúcim prevody môže byť bežný obchod predávajúci tovar, ktorý má dohodu s korešpondenčným podnikom v inej krajine. Zvyčajne nedochádza k fyzickému pohybu meny a chýba formálnosť, pokiaľ ide o overovanie a vedenie záznamov. Prevod peňazí sa uskutočňuje prostredníctvom kódovaných informácií, ktoré sa odovzdávajú prostredníctvom šekov, kuriérov, listov, faxov, e-mailov, textových správ alebo online chatových systémov, po ktorých nasleduje určitá forma telekomunikačných potvrdení.

AMLA (ANTI-MONEY LAUNDERING AUTHORITY)

Orgán EÚ pre boj proti praniu špinavých peňazí (AMLA) je nový regulačný orgán EÚ zriadený nariadením (EÚ) 2024/1620. AMLA má priamy dohľad nad vybranými finančnými inštitúciami s najvyšším rizikom, koordinuje finančné spravodajské jednotky (FIU) a podporuje harmonizovanú implementáciu rámca AML/CFT v celej EÚ. AMLA so sídlom vo Frankfurte nad Mohanom začala plne fungovať v roku 2025.

ANTI-MONEY LAUNDERING DIRECTIVE (AMLD)

Smernica Európskeho parlamentu a Rady o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí a financovania terorizmu. Smernice AMLD sú transponované do národnej legislatívy členských štátov EÚ a stanovujú minimálne štandardy pre systémy AML/CFT.

Od prijatia prvej smernice v roku 1991 prešiel európsky AML/CFT rámec výrazným vývojom:

- **1AMLD (1991)** – prvá európska AML smernica, zameraná výlučne na pranie výnosov z drogovej trestnej činnosti; zaviedla povinnosť identifikácie klientov a oznamovania podozrivých transakcií.
- **2AMLD (2001)** – rozšírila okruh predikátnych trestných činov nad rámec drog; zahrnula ďalšie povinné subjekty (advokáti, notári, účtovníci, realitní makléri).
- **3AMLD (2005)** – implementovala revidované 40 odporúčaní FATF z roku 2003; zaviedla prístup založený na riziku (risk-based approach), hĺbkovú previerku klienta (CDD/EDD/SDD) a pojem politicky exponovanej osoby (PEP).
- **4AMLD (2015)** – posilnila prístup založený na riziku; zaviedla povinnosť registrov skutočných vlastníkov (beneficial ownership) pre právnické osoby a trusty; rozšírila okruh povinných subjektov.
- **5AMLD (2018)** – reagovala na riziká virtuálnych mien a predplatených kariet; sprístupnila registre skutočných vlastníkov verejnosti; posilnila požiadavky na korešpondenčné bankovníctvo a vysokorizikové tretie krajiny.
- **6AMLD (2018, účinná od 2021)** – harmonizovala definíciu trestného činu prania špinavých peňazí v celej EÚ; rozšírila okruh predikátnych trestných činov na 22 kategórií vrátane kybernetickej kriminality a environmentálnych trestných činov; zaviedla trestnú zodpovednosť právnických osôb.

Paralelne s týmto vývojom EÚ prijala v roku 2024 nový balík AML/CFT legislatívy, ktorý nahrádza smernicový prístup priamo aplikovateľným nariadením (AMLAR) a zriaďuje centrálny dohľadový orgán AMLA, čím sa európsky AML/CFT rámec zásadne transformuje.

ANTI-MONEY LAUNDERING INTERNATIONAL DATABASE (AMLID)

Medzinárodnú databáza o boji proti praniu špinavých peňazí (AMLID), ktorá je zbierkou analýz zákonov a predpisov o boji proti praniu špinavých peňazí vrátane dvoch všeobecných tried opatrení na kontrolu prania špinavých peňazí (vnútroštátne zákony a medzinárodná spolupráca), ako aj informácií o vnútroštátnych kontaktoch a orgánoch. AMLID je zabezpečená, viacjazyčná databáza a predstavuje dôležitý referenčný nástroj pre pracovníkov orgánov činných v trestnom konaní, ktorí sa podieľajú na práci medzi jednotlivými jurisdikciami. Dotazník AMLID bol aktualizovaný s cieľom zohľadniť nové trendy a normy v oblasti prania špinavých peňazí a zohľadňuje ustanovenia týkajúce sa financovania terorizmu a ďalšie aktuálne normy, ako sú revidované odporúčania FATF 40 + 9. Okrem toho revidovaný dotazník AMLID teraz obsahuje časť Rámcových dohovorov. Tento poskytuje prehľad o štatúte krajiny alebo územia k medzinárodným dohovorom, ktoré sa vzťahujú na boj proti praniu špinavých peňazí/financovaniu terorizmu *(AML/CFT),* ako aj o štatúte krajiny alebo územia k dvojstranným/viacstranným zmluvám alebo dohodám o vzájomnej právnej pomoci v trestných veciach a vydávaní osôb; ďalej obsahuje referenčnú časť, ktorá obsahuje podrobnosti o najnovšom výskume OSN, abstrakty najlepších nových výskumov vlád a medzinárodných organizácií a bibliografiu; mapu, ktorá používateľov presmeruje na regionálne zoznamy vnútroštátnych právnych predpisov. Táto časť bude obsahovať aj úplné znenie alebo odkazy na úplné znenie všetkých vnútroštátnych právnych predpisov a nariadení v oblasti boja proti praniu špinavých peňazí/financovaniu terorizmu (AML/CFT) na celom svete. Databáza v súčasnosti obsahuje právne predpisy z približne 163 jurisdikcií a od januára 2005 bolo do nej zaradených viac ako 250 nových/zmenených právnych predpisov a nariadení v oblasti boja proti praniu špinavých peňazí/financovaniu terorizmu. AMLID ďalej obsahuje Medzinárodné normy a štandardy: vzorové

zákony pre systémy common law a civil law, normy, dohovory a právne nástroje; celosvetový kalendár podujatí, ktorý obsahuje zoznam aktuálnych vzdelávacích podujatí a konferencií na národnej, regionálnej a medzinárodnej úrovni; a sekciu odkazov, ktorá obsahuje odkazy na webové stránky súvisiacich regionálnych organizácií pôsobiacich v oblasti AML/CFT a finančných spravodajských jednotiek (FIU).

ANTI-MONEY LAUNDERING PROGRAM

Systém vnútorných opatrení, kontrolných mechanizmov a postupov určený na predchádzanie zneužívaniu inštitúcie na účely prania špinavých peňazí a financovania terorizmu. AML program nie je len interným dokumentom – je zákonnou povinnosťou vyplývajúcou z národnej legislatívy, ktorá transponuje medzinárodné štandardy (odporúčania FATF, smernice AMLD v EÚ, Bank Secrecy Act v USA a ekvivalentné predpisy v iných jurisdikciách).

Povinnosť zaviesť AML program sa vzťahuje na širokú skupinu tzv. povinných osôb (obliged entities), ktorá zahŕňa nielen banky a iné úverové inštitúcie, ale aj obchodníkov s cennými papiermi, poisťovne, podniky poskytujúce peňažné služby (MSB), zmenárne, správcov majetku, realitných maklérov, advokátov, notárov, účtovníkov, audítorov, poskytovateľov služieb virtuálnych/krypto aktív (VASP/CASP) a ďalšie subjekty definované príslušnou jurisdikciou.

Efektívny AML program musí obsahovať minimálne štyri základné piliere:

1. **Písomné interné zásady, postupy a kontrolné mechanizmy** – zdokumentovaný rámec upravujúci identifikáciu a overovanie klientov (KYC/CDD), hodnotenie rizík, monitorovanie transakcií, oznamovanie podozrivých aktivít a uchovávanie záznamov.

2. **Určený pracovník zodpovedný za dodržiavanie predpisov** – v závislosti od jurisdikcie označovaný ako Compliance Officer, Money Laundering Reporting Officer (MLRO) alebo Sanctions Compliance Officer (SCO); táto osoba nesie priamu zodpovednosť za implementáciu a aktualizáciu programu.

3. **Priebežné školenia zamestnancov** – pravidelné vzdelávanie zamerané na rozpoznávanie varovných signálov (red flags), typológií prania špinavých peňazí a povinností pri oznamovaní podozrivých aktivít.

4. **Nezávislá kontrola (audit)** – pravidelné testovanie účinnosti programu vykonávané interným auditom alebo nezávislým externým subjektom s cieľom identifikovať slabé miesta a zabezpečiť súlad s aktuálnymi regulačnými požiadavkami.

V EÚ je obsah a rozsah AML programu bližšie špecifikovaný v smerniciach AMLD a súvisiacich usmerneniach EBA. V USA stanovuje minimálne požiadavky Bank Secrecy Act (BSA) a nadväzujúce predpisy FinCEN. Napriek rozdielom medzi jurisdikciami platí spoločný princíp: AML program musí byť primeraný veľkosti, povahe a rizikovému profilu inštitúcie – prístup „jedna veľkosť pre všetkých" regulátori explicitne odmietajú.

ARREST WARRANT

Súdny príkaz, ktorý nariaďuje príslušníkovi orgánu činného v trestnom konaní, aby zaistil a zadržal konkrétnu osobu a požiadal ju, aby odpovedala na sťažnosť alebo sa inak dostavila na súd alebo iný príslušný orgán.

ASIA/PACIFIC GROUP ON MONEY LAUNDERING (APG)

Ázijsko-tichomorská skupina pre pranie špinavých peňazí je medzivládna organizácia, ktorú tvorí 41 členských štátov. Cieľom APG je zabezpečiť, aby jednotliví členovia účinne uplatňovali medzinárodné normy proti praniu špinavých peňazí, financovaniu terorizmu a financovaniu šírenia zbraní hromadného ničenia.

ASSET

Všetko, čo vlastní fyzická alebo právnická osoba a čo má peňažnú hodnotu. Dlhodobý majetok zahŕňa položky ako budovy a zariadenia, ktoré sa využívajú počas dlhšieho obdobia; obežný majetok zahŕňa suroviny, hotovosť a pohľadávky voči tretím stranám.

V kontexte AML/CFT má pojem „majetok" zásadný a oveľa širší význam. Nejde len o ekonomickú kategóriu – majetok je ústredným objektom celého procesu prania špinavých peňazí a financovania terorizmu, a preto jeho vymedzenie v AML/CFT legislatíve úmyselne zahŕňa čo najširší okruh hodnôt. Podľa odporúčaní FATF a smerníc AMLD sa za majetok považujú aktíva akéhokoľvek druhu – hmotné aj nehmotné, hnuteľné aj nehnuteľné, právne dokumenty a listiny preukazujúce vlastníctvo alebo práva k takýmto aktívam, vrátane virtuálnych aktív a kryptomien.

Toto rozšírené chápanie má priamy dopad na niekoľko kľúčových oblastí AML/CFT praxe. Pri identifikácii skutočného vlastníka (beneficial ownership) sa skúma, kto je skutočným vlastníkom alebo ovládajúcou osobou majetku bez ohľadu na to, ako je formálne štruktúrované jeho držanie – práve zložité vlastnícke štruktúry slúžia na zatajenie skutočného pôvodu majetku. Pri zmrazení, zaistení a konfiškácii majetku (asset freezing, seizing, confiscation) je presné vymedzenie pojmu kľúčové pre výkon príkazov zo strany orgánov činných v trestnom konaní a pre plnenie sankčných povinností. Pri posudzovaní pôvodu majetku (source of wealth) a pôvodu finančných prostriedkov (source of funds) – čo sú povinné súčasti hĺbkovej previerky pri rizikovejších klientoch – sa hodnotí celý majetok klienta, nielen konkrétna transakcia.

Osobitnou kategóriou sú v súčasnosti virtuálne aktíva, ktoré FATF explicitne zaradil pod pojem „majetok" a ktorých správa a prevod podliehajú rovnakým AML/CFT povinnostiam ako tradičné formy majetku.

ASSET BLOCKING (BLOKOVANIE MAJETKU)

Postup, ktorým sa fyzickej alebo právnickej osobe odoberie prístup k jej aktívam – spravidla na základe sankčného príkazu, rozhodnutia súdu alebo príslušného orgánu. Blokovanie aktív sa označuje aj ako zmrazenie aktív (asset freezing) a tieto pojmy sa v praxi používajú ako synonymá.

V bežnom právnom chápaní ide o dočasné obmedzenie dispozičného práva s majetkom, ktoré neznamená jeho prepadnutie – vlastník formálne zostáva vlastníkom, avšak nemôže s majetkom nakladať, prevádzať ho, využívať ani inak s ním disponovať až do ďalšieho rozhodnutia príslušného orgánu.

V kontexte AML/CFT a sankčného práva má blokovanie majetku tri odlišné právne základy, ktoré je dôležité rozlišovať:

Sankčné zmrazenie – automatická povinnosť vyplývajúca priamo zo sankčných nariadení (OSN, EÚ, OFAC a iné); finančná inštitúcia je povinná zablokovať majetok okamžite po identifikácii sankcionovanej osoby alebo subjektu, bez čakania na súdny príkaz. Ide o najprísnejší a časovo najnaliehavejší typ.

Procesné zaistenie – nariadené orgánmi činnými v trestnom konaní v rámci vyšetrovania trestného činu prania špinavých peňazí alebo predikátneho trestného činu; slúži na zabezpečenie majetku pre prípadnú neskoršiu konfiškáciu.

Predbežné opatrenie – nariadené súdom v civilnom alebo správnom konaní na zabezpečenie nárokov poškodených strán.

Pre finančné inštitúcie vyplývajú z blokovania majetku konkrétne povinnosti: okamžité zmrazenie prostriedkov na účtoch, zákaz vykonávania akýchkoľvek transakcií v prospech alebo na ťarchu blokovaného majetku, povinnosť oznámiť blokovanie príslušnému sankčnému orgánu (v EÚ národnému príslušnému orgánu, v USA OFAC) a pravidelné reportovanie o blokovanom

majetku. Porušenie povinnosti blokovať majetok sankcionovanej osoby predstavuje jedno z najzávažnejších porušení sankčných predpisov s potenciálne vysokými sankciami pre inštitúciu aj zodpovedné fyzické osoby.

ASSET CONFISCATION

Postup, ktorým štát alebo príslušný orgán trvalo prevezme vlastníctvo majetku fyzickej alebo právnickej osoby. Na rozdiel od blokovania alebo zmrazenia majetku, ktoré sú dočasné a vlastníctvo formálne zachovávajú, konfiškácia znamená definitívny a nezvratný prechod vlastníckeho práva na štát.

V bežnom právnom chápaní ide o sankciu alebo procesný inštitút, ktorý nasleduje po právoplatnom rozhodnutí súdu alebo príslušného orgánu. Konfiškácia sa tradične chápe ako trest alebo následok protiprávneho konania.

V kontexte AML/CFT a sankčného práva je konfiškácia jedným z najsilnejších nástrojov odnímania nezákonne nadobudnutého majetku a zároveň kľúčovým prvkom odstrašujúceho účinku celého systému. Rozlišujeme niekoľko zásadne odlišných foriem:

Trestnoprávna konfiškácia (conviction-based confiscation) – najrozšírenejšia forma; majetok je konfiškovaný ako priamy dôsledok právoplatného odsúdenia za trestný čin prania špinavých peňazí alebo predikátny trestný čin. Vyžaduje preukázanie viny za trestný čin.

Konfiškácia bez odsúdenia (non-conviction based confiscation, NCB) – majetok je konfiškovaný v občianskoprávnom alebo správnom konaní bez nutnosti trestného odsúdenia vlastníka; štát preukazuje, že majetok pochádza z trestnej činnosti alebo je s ňou spojený. FATF tento nástroj aktívne odporúča ako efektívny spôsob odnímania výnosov z trestnej činnosti najmä v prípadoch, keď trestné stíhanie nie je možné.

Sankčná konfiškácia – v niektorých jurisdikciách (najmä USA) môže OFAC nariadiť konfiškáciu majetku sankcionovaných subjektov aj bez trestného konania, na základe sankčných nariadení.

Správna konfiškácia – vykonávaná colnými alebo inými správnymi orgánmi, typicky pri fyzickom prevoze hotovosti cez hranice bez splnenia oznamovacej povinnosti.

Pre finančné inštitúcie je konfiškácia relevantná najmä z hľadiska spolupráce s orgánmi činnými v trestnom konaní pri výkone konfiškačných príkazov, povinnosti zablokovať majetok pred jeho konfiškáciou a medzinárodnej spolupráce pri cezhraničnej konfiškácii výnosov z trestnej činnosti. Práve efektívna konfiškácia je podľa FATF jedným z najdôležitejších meradiel funkčnosti celého AML/CFT systému krajiny – systém, ktorý neumožňuje páchateľom odňať výnosy z trestnej činnosti, stráca odstrašujúci účinok.

ASSET FLIGHT

Presun majetku z jednej jurisdikcie do druhej s cieľom vyhnúť sa právnym dôsledkom – pokutám, konfiškácii, sankciám alebo iným opatreniam príslušných orgánov. V bežnom chápaní môže ísť aj o legálnu optimalizáciu daňového zaťaženia alebo ochranu majetku pred politickou nestabilitou; hranica medzi legálnym a nelegálnym presunom majetku je preto v praxi často predmetom právneho posúdenia.

V kontexte AML/CFT predstavuje asset flight závažný typologický vzorec, ktorý priamo narúša účinnosť celého systému boja proti praniu špinavých peňazí. Ide spravidla o reakciu na hroziace vyšetrovanie, zmrazenie majetku alebo sankčné opatrenia – páchatelia sa snažia presunúť majetok skôr, než príslušné orgány stihnú konať. Práve preto odporúčania FATF kladú dôraz na rýchlosť zmrazenia majetku a požadujú, aby k nemu dochádzalo „bez zbytočného odkladu" (without delay).

Typické techniky asset flight zahŕňajú prevod majetku na spriaznené osoby alebo bábkové spoločnosti (straw man, shell company) v zahraničných jurisdikciách s slabým AML/CFT rámcom, využívanie nepriehľadných vlastníckych štruktúr na zatajenie skutočného vlastníka, prevod nehnuteľností a iných aktív tesne pred začatím vyšetrovania, fyzický export hotovosti alebo drahých kovov cez hranice a konverziu majetku do virtuálnych aktív, ktoré umožňujú rýchly cezhraničný presun mimo dosahu tradičných finančných systémov.

Pre finančné inštitúcie je rozpoznanie varovných signálov asset flight kľúčovou súčasťou monitorovania transakcií. Medzi typické red flags patrí náhle zvýšenie objemu odchádzajúcich medzinárodných prevodov, urýchlené ukončovanie obchodných vzťahov, predaj nehnuteľností a iných aktív za ceny výrazne pod trhovou hodnotou, prevozy do jurisdikcií na zozname FATF alebo jurisdikcií bez účinných extradičných zmlúv a neobvyklý záujem klienta o diskrétnosť pri prevodoch. Podozrenie na asset flight zakladá povinnosť podania oznámenia o podozrivej aktivite (SAR/STR) a môže byť základom pre bezodkladné zmrazenie majetku.

ASSET FORFEITURE (PREPADNUTIE MAJETKU)

Právny nástroj, ktorým štát trvalo odníma majetok spojený s trestnou činnosťou alebo pochádzajúci z nej. Spolu s konfiškáciou (asset confiscation) patrí prepadnutie majetku k najúčinnejším prostriedkom odnímania výnosov z trestnej činnosti a narúšania finančnej základne organizovaného zločinu – páchateľ prichádza nielen o slobodu, ale aj o ekonomický prospech zo svojej trestnej činnosti.

Hoci sa pojmy asset forfeiture a asset confiscation v praxi často používajú ako synonymá, v anglosaskom právnom systéme sa tradične rozlišujú dva základné typy prepadnutia majetku:

Trestnoprávne prepadnutie majetku (criminal forfeiture) – majetok prepadá ako priamy dôsledok trestného odsúdenia páchateľa; je namierené proti osobe (in personam) a vyžaduje preukázanie viny za trestný čin nad rámec rozumnej pochybnosti. Vzťahuje sa na majetok priamo použitý pri páchaní trestného činu alebo získaný jeho spáchaním.

Občianskoprávne prepadnutie majetku (civil forfeiture) – konanie je vedené priamo proti majetku (in rem), nie proti jeho vlastníkovi; na prepadnutie postačuje preukázanie spojitosti majetku s trestnou činnosťou na úrovni prevažujúcej pravdepodobnosti, pričom trestné odsúdenie vlastníka nie je podmienkou. Ide o mimoriadne účinný nástroj najmä v prípadoch, keď páchateľa nie je možné trestne stíhať – napríklad pri úteku, smrti alebo nedostatku dôkazov pre trestné konanie.

V kontexte AML/CFT je prepadnutie majetku priamo previazané s povinnosťami finančných inštitúcií: blokovanie majetku pred jeho prepadnutím na základe príkazu orgánov, spolupráca pri identifikácii a sledovaní majetku určeného na prepadnutie a plnenie oznamovacích povinností voči príslušným orgánom. FATF považuje efektívne využívanie inštitútu prepadnutia majetku za jeden z kľúčových ukazovateľov funkčnosti národného AML/CFT systému.

ASSET FREEZING

Zabránenie osobe, na ktorú sa vzťahujú sankcie, v prístupe k jej bankovému účtu alebo iným finančným aktívam alebo v ich používaní. Zmrazenie aktív sa označuje aj ako blokovanie aktív. Viď. definíciu Asset Blocking.

ASSET MINGLING

Nezákonná prax zámerného spájania finančných prostriedkov alebo majetku pochádzajúceho z trestnej činnosti s legálnymi zdrojmi s cieľom zastrieť nelegálny pôvod a sťažiť jeho identifikáciu a sledovanie. Typickým príkladom je nákup nehnuteľností, podnikov alebo iných aktív s použitím kombinácie legálnych a nelegálnych finančných prostriedkov.

V bežnom chápaní môže ísť zdanlivo o štandardnú obchodnú transakciu – napríklad kúpa nehnuteľnosti financovaná kombináciou hypotekárneho úveru a vlastných zdrojov. Práve táto podoba s legitímnymi transakciami robí asset mingling obzvlášť ťažko odhaliteľným.

V kontexte AML/CFT predstavuje asset mingling klasickú techniku fázy vrstenia (layering) alebo integrácie (integration) v procese prania špinavých peňazí. Miešaním zdrojov páchateľ sleduje niekoľko cieľov súčasne: znižuje pomer nelegálnych prostriedkov v celkovej hodnote aktíva, vytvára zdanie legitímneho financovania, komplikuje orgánom sledovanie a preukázanie nelegálneho pôvodu prostriedkov a sťažuje prípadnú konfiškáciu, keďže majetok nie je financovaný výlučne z nelegálnych zdrojov.

Najčastejšie využívané techniky zahŕňajú nákup nehnuteľností s kombináciou hotovosti neznámeho pôvodu a hypotekárneho úveru, vkladanie nelegálnych príjmov do cash-intensive businesses (reštaurácie, práčovne, parkoviská) spolu s legitímnymi tržbami, investície do podnikov, kde sú nelegálne prostriedky prezentované ako podnikateľský zisk, a využívanie zložitých firemných štruktúr, kde sa nelegálne prostriedky miešajú s kapitálovými vkladmi legitímnych spoločníkov.

Pre finančné inštitúcie je rozpoznanie asset mingling náročné, avšak kriticky dôležité. Medzi typické varovné signály patrí neobvyklá kombinácia zdrojov financovania pri významných transakciách, nepomer medzi deklarovanými príjmami klienta a hodnotou nadobúdaného majetku, využívanie hotovosti alebo prevodov z nejasných zdrojov ako časti financovania, časté prepájanie osobných a firemných financií a transakcie prechádzajúce cez viaceré jurisdikcie bez zjavného obchodného dôvodu. Pri podozrení na asset mingling vzniká povinnosť podania oznámenia o podozrivej aktivite (SAR/STR) a v závislosti od okolností aj povinnosť zvážiť ukončenie obchodného vzťahu.

ASSET PROTECTION

Proces zahŕňajúci reorganizáciu spôsobu držby majetku s cieľom znížiť jeho zraniteľnosť voči potencionálnym nárokom veriteľov, súdnym rozhodnutiam alebo iným právnym záväzkom. V daňovom plánovaní sa tento pojem používa aj pre opatrenia prijímané na ochranu majetku pred zdanením v iných jurisdikciách.

V bežnom právnom a finančnom chápaní je ochrana majetku legitímnou disciplínou – fyzické aj právnické osoby majú právo štruktúrovať držbu svojho majetku spôsobom, ktorý minimalizuje právne a finančné riziká. Bežne využívané nástroje zahŕňajú trusty, holdingové spoločnosti, poistné produkty či manželské majetkové zmluvy.

V kontexte AML/CFT však ochrana majetku predstavuje jednu z najvýznamnejších šedých zón, kde sa legitímne plánovanie stretáva s potencionálnym zneužitím na účely prania špinavých peňazí, daňových únikov a obchádzania sankcií. Kľúčovou otázkou pre finančné inštitúcie a orgány dohľadu nie je samotné použitie nástrojov ochrany majetku, ale účel, ktorému slúžia, a transparentnosť ich štruktúry.

Medzi typické techniky zneužitia ochrany majetku na účely prania špinavých peňazí patrí prevod majetku do trustov alebo nadácií v jurisdikciách s vysokou mierou utajenia skutočného vlastníka, využívanie Asset Protection Trustov (APT) v offshore jurisdikciách na odstrihnutie majetku od jeho skutočného vlastníka, vkladanie majetku do zložitých viacúrovňových štruktúr spoločností s cieľom nemožniť identifikáciu skutočného vlastníka *(beneficial owner)* či fiktívne prevody majetku na rodinných príslušníkov alebo spriaznené osoby *(sham divestment)* bezprostredne pred začatím vyšetrovania alebo sankčného konania.

Pre finančné inštitúcie vyplývajú z tejto problematiky konkrétne povinnosti: pri klientoch využívajúcich komplexné štruktúry ochrany majetku je nevyhnutná dôkladná hĺbková previerka (EDD) zameraná na identifikáciu konečného užívateľa výhod, overenie legitímnosti účelu štruktúry a posúdenie, či nejde o zastretý pokus o zatajenie pôvodu majetku alebo obchádzanie zákonných povinností. Samotná existencia štruktúry ochrany majetku nie je automaticky varovným signálom – avšak odmietanie transparentnosti, nejasný obchodný účel alebo prepojenie na jurisdikcie s vysokým rizikom AML/CFT sú okolnosti, ktoré zvyšujú rizikový profil klienta a vyžadujú osobitný prístup.

ASSET PROTECTION TRUSTS (APTS)

Osobitná forma neodvolateľného trustu (zverenecký fond), ktorý sa zvyčajne vytvára (t. j. zriaďuje) v zahraničí s hlavným cieľom zachovať a chrániť časť majetku pred veriteľmi. Vlastnícke právo k majetku sa prevedie na osobu menovanú ako správca *(trustee)*. APT sa zvyčajne používajú na ochranu majetku a sú zvyčajne daňovo neutrálne. Ich konečnou funkciou je zabezpečiť príjemcov. Niektorí zástancovia propagujú APT ako nástroj, ktorý umožňuje zahraničným správcom ignorovať súdne príkazy a jednoducho previesť trust do inej jurisdikcie v reakcii na právne kroky ohrozujúce majetok trustu.

ASSET RECOVERY

Proces identifikácie, zmrazenia, zaistenia, konfiškácie a vrátenia výnosov z trestnej činnosti alebo iného neoprávnene nadobudnutého majetku. Vrátenie majetku je kľúčovým prvkom UNCAC (Dohovor OSN proti korupcii) a zahŕňa mechanizmy medzinárodnej spolupráce na cezhraničné sledovanie a repatriáciu majetku.

ASSET TRACING

Vyšetrovacia technika na identifikáciu a sledovanie majetku pochádzajúceho z trestnej činnosti prostredníctvom komplexných finančných vyšetrovaní. Zahŕňa analýzu bankových záznamov, firemných štruktúr, nehnuteľností a iných aktív s cieľom preukázať vlastníctvo a pôvod finančných prostriedkov.

AUTOMATED CLEARING HOUSE (ACH)

Sieť ACH je elektronický systém, ktorý slúži finančným inštitúciám na uľahčenie finančných transakcií v USA. Zastupuje viac ako 10 000 finančných inštitúcií a transakcie ACH dosiahli v roku 2023 celkovú hodnotu viac ako 80,1 bilióna USD tým, že umožnili viac ako 31,5 miliárd elektronických finančných transakcií. Sieť v podstate funguje ako finančné centrum a pomáha ľuďom a organizáciám presúvať peniaze z jedného bankového účtu na druhý. Transakcie ACH pozostávajú z vkladov a platieb, vrátane transakcií medzi podnikmi (B2B), vládnych transakcií, ako aj spotrebiteľských transakcií.

AUTOMATED SCREENING TOOL (AST)

Softvérové systémy používané veľkými finančnými inštitúciami na uľahčenie procesu preverovania na rozdiel od manuálneho preverovania. Systémy AST sú vo všeobecnosti navrhnuté tak, aby kontrolovali zoznamy sankcií. Systémy AST generujú pozitívne lustrácie na základe sankčných zoznamov, ktoré sa môžu konsolidovať do upozornení *(Alerts)* napríklad na základe záznamu o klientovi. V prípade jedného záznamu o klientovi môže byť viacero pozitívnych lustrácií na základe sankčných zoznamov, ktoré sú konsolidované v rámci jedného upozornenia.

AUTOMATED TELLER MACHINE (ATM)

Elektronické bankové pracovisko, ktoré umožňuje klientom vykonávať základné transakcie bez asistencie zamestnanca banky. Bankomaty spravidla vydávajú hotovosť, umožňujú vkladať šeky a hotovosť a vykonávať prevody, ako aj zisťovať zostatok.

V bežnom chápaní ide o súčasť štandardnej bankovej infraštruktúry, ktorá zvyšuje dostupnosť finančných služieb a znižuje záťaž pobočkových sietí. Bankomaty prevádzkujú nielen banky, ale aj nezávislí prevádzkovatelia *(IAD – Independent ATM Deployers),* čo má priamy dopad na úroveň AML/CFT kontroly nad týmito zariadeniami.

V kontexte AML/CFT predstavujú bankomaty špecifický rizikový kanál, a to najmä z dôvodu hotovostného charakteru transakcií a obmedzenej možnosti priamej identifikácie používateľa v reálnom čase. Medzi najčastejšie zneužívané techniky patrí štruktúrovanie vkladov hotovosti *(smurfing)* prostredníctvom série vkladov na rôznych bankomatoch pod hranicou povinného hlásenia, využívanie bankomatov tretích strán na anonymné výbery v jurisdikciách s nižšou úrovňou AML/CFT kontroly, pranie špinavých peňazí prostredníctvom vopred nabitých platobných kariet *(Prepaid Cards),* ktoré sú dobíjané z nelegálnych zdrojov a vyberané cez bankomaty, a využívanie bankomatov akceptujúcich kryptomeny (Bitcoin ATM) na konverziu virtuálnych aktív na hotovosť s minimálnymi požiadavkami na identifikáciu. Osobitnou rizikovou kategóriou sú práve tieto kryptomenové bankomaty (crypto ATM), ktorých počet v posledných rokoch výrazne rastie. FATF a národné regulačné orgány im venujú zvýšenú pozornosť, keďže historicky fungovali s minimálnymi požiadavkami na KYC – situácia, ktorú regulátori v EÚ aj v USA postupne napravujú sprísňovaním požiadaviek na prevádzkovateľov.

Pre finančné inštitúcie vyplývajú z prevádzky bankomatov konkrétne AML/CFT povinnosti: monitorovanie neobvyklých vzorcov transakcií (časté vklady pod reportingovou hranicou, opakované výbery na rôznych miestach v krátkom čase), due diligence voči nezávislým prevádzkovateľom bankomatov ako voči obchodným partnerom a zabezpečenie, že bankomaty neumožňujú anonymné transakcie nad zákonom stanovené limity.

BACK-TO-BACK LETTERS OF CREDIT

Forma financovania, pri ktorej banka A vystaví akreditív ako zábezpeku banke B, aby mohla vystaviť samostatný akreditív príjemcovi. Často sa to stáva, keď základná zmluva medzi žiadateľom a príjemcom obsahuje obmedzenia týkajúce sa úverovej kvality banky, ktorá vystavuje akreditív, umiestnenia vystavujúcej banky alebo iné ustanovenia, ktoré bránia banke žiadateľa vystaviť priamy akreditív príjemcovi. Subjekt, ktorý sa vyhýba sankciám, môže použiť akreditív typu back-to-back, aby z dokumentácie odstránil názov banky, na ktorú sa vzťahujú sankcie.

BANK DRAFT

Pojem zmenka/šek označuje obchodovateľný nástroj, ktorý možno použiť ako platidlo rovnako ako šek. Na rozdiel od šeku však za bankovú zmenku ručí banka, ktorá ju vystavila. Celková suma zmenky sa čerpá z účtu žiadajúceho platiteľa - zostatok jeho bankového účtu sa znižuje o peniaze stiahnuté z účtu - a zvyčajne sa drží na účte hlavnej knihy, kým príjemca platby zmenku nepreplatí. Bankové zmenky poskytujú príjemcovi platby bezpečnú formu platby. Je zraniteľná v oblasti AML/CFT, pretože predstavuje renomovaný medzinárodný peňažný nástroj vystavený renomovanou inštitúciou a často je splatný v hotovosti po predložení a na účte vydávajúcej inštitúcie v inej krajine.

BANK SECRECY

Vzťahuje sa na zákony a nariadenia v krajinách, ktoré zakazujú bankám zverejňovať informácie o účte alebo dokonca odhaliť jeho existenciu bez súhlasu majiteľa účtu. Bráni cezhraničnému toku informácií medzi finančnými inštitúciami a ich orgánmi dohľadu.

BANK SECRECY ACT (BSA)

Hlavný regulačný zákon USA proti praniu špinavých peňazí (Hlava 31, Zákonník USA, oddiely 5311-5355), ktorý bol prijatý v roku 1970 a najvýraznejšie zmenený zákonom USA Patriot Act v roku 2001. Okrem iných opatrení ukladá finančným inštitúciám a mnohým ďalším podnikom kontrolu prania špinavých peňazí vrátane povinnosti podávať správy a viesť záznamy o rôznych finančných transakciách.

BANK SECRECY ACT COMPLIANCE PROGRAM

Program, ktorý sú finančné inštitúcie so sídlom v USA - v zmysle zákona o bankovom tajomstve - povinné zaviesť a implementovať s cieľom kontrolovať pranie špinavých peňazí a súvisiace finančné trestné činy. Medzi zložky programu patrí minimálne: vypracovanie interných zásad, postupov a kontrolných mechanizmov, vymenovanie pracovníka zodpovedného za dodržiavanie predpisov, priebežné školenie zamestnancov a nezávislý audit na testovanie programu.

BASEL COMMITTEE ON BANKING SUPERVISION (BASEL COMMITTEE)

Bazilejský výbor založili guvernéri centrálnych bánk krajín skupiny G-10 v roku 1974 s cieľom podporovať spoľahlivé štandardy dohľadu na celom svete. Jeho sekretariát vymenúva Banka pre medzinárodné zúčtovanie v Bazileji vo Švajčiarsku. Okrem iného vydal dokumenty o povinnej starostlivosti bánk vo vzťahu ku klientovi, konsolidovanom riadení rizík KYC, transparentnosti platobných správ, povinnej starostlivosti a transparentnosti v súvislosti s krycími platobnými správami týkajúcimi sa cezhraničných prevodov a zdieľaní finančných záznamov medzi jurisdikciami v súvislosti s bojom proti financovaniu terorizmu.

BATCH TRANSFER

Prevod pozostávajúci z viacerých jednotlivých bankových prevodov zoskupených do jednej skupiny (dávky), ktoré sú odosielané do rovnakej finančnej inštitúcie, pričom môžu, ale nemusia byť určené pre rôznych príjemcov. Hromadné prevody sa bežne využívajú napríklad pri výplate miezd, úhrade dodávateľských faktúr alebo spracovaní hromadných platieb v rámci podnikových procesov.

V bežnom bankovom prostredí ide o štandardný a efektívny spôsob spracovania veľkého počtu platieb, ktorý znižuje prevádzkové náklady a zjednodušuje administráciu opakujúcich sa transakcií.

V kontexte AML/CFT predstavujú hromadné prevody špecifickú výzvu, ktorá vyplýva priamo z ich technickej podstaty. Kľúčovým problémom je, že v hromadnom prevode môžu byť individuálne transakcie zbavené informácií o príkazcovi a príjemcovi, ktoré by inak sprevádzali každý samostatný prevod. Toto je v priamom rozpore s požiadavkami na transparentnosť platieb podľa odporúčania FATF č. 16 (Travel Rule) a nariadenia EÚ o transfere fondov (2023/1113), ktoré vyžadujú, aby každý prevod sprevádzali úplné a presné informácie o príkazcovi a príjemcovi.

Finančné inštitúcie spracúvajúce hromadné prevody sú povinné zabezpečiť, že aj napriek hromadnému charakteru spracovania sú pre každú individuálnu transakciu v dávke dostupné a overiteľné identifikačné údaje o príkazcovi a príjemcovi, systémy monitorovania transakcií sú schopné analyzovať jednotlivé platby v rámci dávky a nielen dávku ako celok, a neobvyklé vzorce v hromadných prevodoch – napríklad neštandardná frekvencia, neobvyklí príjemcovia alebo nekonzistentné sumy – sú správne identifikované a vyhodnotené.

Hromadné prevody sú tiež potenciálnym nástrojom zneužitia pri štruktúrovaní platieb, keď páchatelia rozkladajú väčšie sumy do množstva menších prevodov spracovaných v jednej dávke práve s cieľom vyhnúť sa prekročeniu hraníc povinného hlásenia a automatickým kontrolám monitorovacích systémov.

BATCH PROCESSING

Typ spracovania údajov a prenosu dát, pri ktorom sa súvisiace transakcie

zoskupujú a prenášajú na spracovanie, zvyčajne tým istým počítačom a v rámci tej istej aplikácie. Taktiež viď. definíciu Batch Transfer.

BATCH SCREENING

Proces pravidelného preverovania celej zákazníckej základne firmy a ďalších pridružených subjektov, ako sú dodávatelia, pomocou AST. Taktiež viď. definíciu Batch Transfer.

BEARER FORM (FORMA NA DORUČITEĽA)

Právna forma cenného papiera, investičného nástroja alebo dokumentu, pri ktorej sa vlastníctvo viaže výlučne na fyzické držanie listiny – vlastníkom je ten, kto dokument fyzicky drží, bez ohľadu na to, či je jeho meno kdekoľvek zaznamenané. Prevod vlastníctva sa uskutočňuje samotným odovzdaním listiny, bez potreby písomných pokynov, registrácie, alebo súhlasu emitenta.

V bežnom finančnom a obchodnom prostredí bola forma na doručiteľa historicky rozšíreným nástrojom pre akcie, dlhopisy, šeky a iné cenné papiere, keďže umožňovala jednoduchý a rýchly prevod vlastníctva bez administratívnej záťaže.

V kontexte AML/CFT predstavuje táto forma jeden z najvyššie rizikových nástrojov aké finančný systém pozná – a práve preto je predmetom intenzívnej regulácie alebo úplného zákazu vo väčšine vyspelých jurisdikcií. Základným problémom je úplná anonymita vlastníctva a to robí nástroje vo forme na doručiteľa ideálnym prostriedkom na pranie špinavých peňazí, daňové úniky, obchádzanie sankcií a skrývanie výnosov z trestnej činnosti.

FATF vo svojich odporúčaniach (najmä č. 24) explicitne požaduje, aby krajiny prijali opatrenia zabraňujúce zneužitiu akcií na doručiteľa a opčných listov na doručiteľa, pričom preferovaným riešením je ich úplné zrušenie alebo povinná imobilizáciu u regulovaného správcu. V EÚ smernice AMLD fakticky viedli k zákazu vydávania nových akcií na doručiteľa vo väčšine členských štátov a k povinnej konverzii existujúcich nástrojov na registrované formy.

Pre finančné inštitúcie predstavuje akýkoľvek kontakt s nástrojmi vo forme na doručiteľa automaticky zvýšené riziko AML/CFT vyžadujúce rozšírenú hĺbkovú previerku (EDD), dôkladné preskúmanie účelu a pôvodu nástroja a v mnohých prípadoch aj podanie oznámenia o podozrivej aktivite. Existencia týchto nástrojov v majetkovej štruktúre klienta je sama o sebe významným varovným signálom.

BEARER NEGOTIABLE INSTRUMENTS (BNIS)

Obchodovateľné nástroje na doručiteľa (BNI) zahŕňajú peňažné nástroje na doručiteľa, ako sú: cestovné šeky; obchodovateľné nástroje (vrátane šekov, zmeniek a peňažných poukážok), ktoré sú buď vo forme na doručiteľa, indosované bez obmedzenia, vystavené na fiktívneho príjemcu, alebo inak v takej forme, že vlastnícke právo k nim prechádza doručením; neúplné nástroje (vrátane šekov, zmeniek a peňažných poukážok) podpísané, ale s vynechaným menom príjemcu. Viď. tiež definíciu Bearer Form.

BEARER SHARE

Obchodovateľné nástroje, ktoré priznávajú vlastníctvo v korporácii osobe, ktorá má fyzicky v držbe podielový list na doručiteľa, podielový list vystavený na "doručiteľa" a nie na meno jednotlivca alebo organizácie. Taktiež akcie na doručiteľa - vzťahujú sa na prevoditeľné nástroje, ktoré priznávajú vlastníctvo v právnickej osobe osobe, ktorá vlastní listinnú akciu na doručiteľa. Viď. tiež definíciu Bearer Form.

BENAMI ACCOUNT

Nazýva sa aj účet na meno. Benamské účty, ktoré vedie jedna osoba alebo subjekt v mene inej osoby alebo iných osôb, sú spojené s „podzemným" bankovým systémom hawala na indickom subkontinente. Osoba v jednej jurisdikcii, ktorá chce presunúť finančné prostriedky prostredníctvom hawaladaru do inej jurisdikcie, môže použiť účet benami alebo transakciu benami na zakrytie svojej skutočnej totožnosti alebo totožnosti príjemcu finančných prostriedkov.

BENEFICIAL OWNER

Pod pojmom skutočný vlastník sa rozumie fyzická osoba (fyzické osoby), ktorá v konečnom dôsledku[1] vlastní alebo kontroluje klienta[2] a/alebo fyzická osoba, v mene ktorej sa transakcia vykonáva. Zahŕňa aj osoby, ktoré vykonávajú konečnú účinnú kontrolu nad právnickou osobou alebo právnym usporiadaním (trustom, nadáciou apod.) a to bez ohľadu na, akými formálnymi prostriedkami je táto kontrola vykonávaná. Vo februári 2022 FATF výrazne revidoval Odporúčanie č. 24 (transparentnosť právnických osôb) – viac nižšie.

V bežnom právnom chápaní sa skutočný vlastník odlišuje od nominálneho vlastníka – teda od osoby, ktorá je formálne zapísaná ako vlastník alebo konateľ, ale koná v mene a na pokyn skutočného vlastníka. Práve tento rozdiel medzi formálnym a skutočným vlastníctvom je jadrom celej problematiky.

V kontexte AML/CFT je identifikácia skutočného vlastníka jednou z najdôležitejších a zároveň najnáročnejších povinností finančných inštitúcií. Páchatelia prania špinavých peňazí, korupcie a daňových únikov systematicky využívajú zložité vlastnícke štruktúry – vrstvenie spoločností, trustov, nominálnych vlastníkov a splnomocnencov – práve s cieľom skryť totožnosť skutočného vlastníka a znemožniť sledovanie majetku a finančných tokov.

Štandardne sa za skutočného vlastníka považuje fyzická osoba, ktorá priamo alebo nepriamo vlastní alebo kontroluje viac ako 25 % podiel v právnickej osobe, pričom mnohé jurisdikcie a inštitúcie pri vyššom rizikovom profile klienta uplatňujú nižší prah (10 % alebo aj menej). Ak nie je možné identifikovať fyzickú osobu spĺňajúcu toto kritérium, za skutočného vlastníka sa považuje senior manažér vykonávajúci skutočnú kontrolu nad inštitúciou.

Vo februári 2022 FATF revidoval odporúčanie č. 24 o transparentnosti právnických osôb a zaviedol niekoľko zásadných zmien. Krajiny sú povinné zabezpečiť uchovávanie informácií o skutočných vlastníkoch v centrálnych registroch, nielen na úrovni samotných spoločností, pričom tieto informácie musia byť aktuálne, presné a prístupné príslušným orgánom. Povinnosť overovania informácií o skutočnom vlastníkovi sa výrazne sprísnila – nestačí pasívne prijať deklaráciu klienta, ale je potrebné aktívne overovať jej pravdivosť prostredníctvom verejných registrov, komerčných databáz a ďalších zdrojov. Zároveň sa rozšírili požiadavky na krajiny s ohľadom na akcie na doručiteľa a nominálnych vlastníkov, ktorí musia byť evidovaní a ich vzťah k skutočnému vlastníkovi musí byť transparentný.

V EÚ tieto požiadavky implementujú smernice AMLD prostredníctvom registrov skutočných vlastníkov *(beneficial ownership registers),* ktoré sú v závislosti od členského štátu čiastočne alebo úplne verejne prístupné. Pre finančné inštitúcie zostáva identifikácia a overovanie skutočného vlastníka jednou z najnáročnejších praktických výziev, a to

[1] Odkaz na "v konečnom dôsledku vlastní alebo kontroluje" a "konečnú účinnú kontrolu" sa vzťahuje na situácie, v ktorých sa vlastníctvo/kontrola vykonáva prostredníctvom vlastníckeho reťazca alebo prostredníctvom inej kontroly ako priamej kontroly.

[2] Táto definícia by sa mala vzťahovať aj na skutočného vlastníka oprávnenej osoby v rámci životného poistenia alebo iného poistenia spojeného s investíciami.

najmä pri komplexných cezhraničných štruktúrach, kde jednotlivé vrstvy vlastníctva prechádzajú viacerými jurisdikciami s rôznymi štandardmi transparentnosti.

BENEFICIAL OWNERSHIP REGISTER

Verejne dostupný alebo prístupný register, ktorý obsahuje informácie o skutočných vlastníkoch právnických osôb a právnych zriadení. V EÚ je povinnosť viesť takéto registre zakotvená v smerniciach AMLD. Registre skutočného vlastníctva zvyšujú transparentnosť a sťažujú využívanie právnických osôb na pranie špinavých peňazí.

BENEFICIARY

Význam pojmu príjemca v odporúčaniach FATF závisí od kontextu. V trustovom práve je beneficient osoba alebo osoby, ktoré majú nárok na prospech z akéhokoľvek trustového usporiadania. Príjemcom môže byť fyzická alebo právnická osoba alebo usporiadanie. Všetky trusty (okrem charitatívnych alebo zákonom povolených necharitatívnych trustov) musia mať zistiteľných príjemcov. Zatiaľ čo trusty musia mať vždy nejakého konečného zistiteľného príjemcu, trusty nemusia mať žiadnych definovaných existujúcich príjemcov, ale len predmety moci, kým sa nejaká osoba nestane oprávnenou ako príjemca na príjem alebo kapitál po uplynutí definovaného obdobia, známeho ako akumulačné obdobie. Toto obdobie je zvyčajne súbežné s obdobím trvania trustu, ktoré sa v zmluve o truste zvyčajne označuje ako obdobie trustu. V kontexte životného poistenia alebo iného poistenia spojeného s investíciami je oprávnenou osobou fyzická alebo právnická osoba, prípadne právne usporiadanie alebo kategória osôb, ktorým budú vyplatené výnosy z poistenia, keď/ak nastane poistná udalosť, na ktorú sa poistenie vzťahuje.

BENEFICIARY FINANCIAL INSTITUTION

Označuje finančnú inštitúciu, ktorá prijíma bankový prevod od príkazcu priamo alebo prostredníctvom sprostredkujúcej finančnej inštitúcie a sprístupňuje finančné prostriedky príjemcovi. V platobnom reťazci vystupuje ako posledný článok na strane príjemcu – jej úlohou je pripísať prostriedky na účet príjemcu alebo ich iným spôsobom dať k dispozícii.

V bežnom bankovom chápaní ide o štandardnú súčasť korešpondenčného bankovníctva a medzinárodných platobných systémov. Prijímajúca finančná inštitúcia nemusí mať s príkazcom žiadny priamy zmluvný vzťah – môže byť zapojená do platobného reťazca výlučne na základe svojho vzťahu s príjemcom.

V kontexte AML/CFT zohráva prijímajúca finančná inštitúcia kľúčovú úlohu v systéme kontroly medzinárodných platieb, pričom jej povinnosti sú priamo zakotvené v odporúčaní FATF č. 16 (Travel Rule) a nariadení EÚ o transfere fondov (2023/1113). Tieto predpisy vyžadujú, aby prijímajúca finančná inštitúcia pri každom prichádzajúcom prevode overila úplnosť a konzistentnosť informácií o príkazcovi a príjemcovi sprevádzajúcich platbu. Ak tieto informácie chýbajú alebo sú neúplné, inštitúcia je povinná prijať primerané opatrenia – požiadať o doplnenie chýbajúcich údajov, obmedziť alebo odmietnuť transakciu a v závislosti od okolností podať oznámenie o podozrivej aktivite *(SAR/STR)*.

Osobitne dôležitou povinnosťou prijímajúcej finančnej inštitúcie je screeningová kontrola príjemcu voči sankčným zoznamom ešte pred pripísaním prostriedkov na jeho účet. Príjemca môže byť sankcionovanou osobou alebo subjektom, a pripísanie prostriedkov na jeho účet – aj keď inštitúcia vystupuje len ako technický sprostredkovateľ – môže predstavovať porušenie sankčných predpisov s vážnymi právnymi a reputačnými následkami.

Prijímajúca finančná inštitúcia nesie zodpovednosť aj za vyhodnotenie rizika platieb prichádzajúcich z korešpondenčných bánk v jurisdikciách s vysokým rizikom AML/CFT alebo zo zdrojov, ktoré nie sú dostatočne preverené. V takýchto prípadoch je nevyhnutné uplatniť zvýšenú mieru obozretnosti a posúdiť, či prichádzajúce platby nevykazujú znaky prania špinavých peňazí, obchádzania sankcií alebo financovania terorizmu.

BILL OF EXCHANGE (ZMENKA)

Prepravný doklad, v ktorom sú uvedené prostriedky, ktorými sa vývozcom platí za tovar, ktorý sa má odoslať, vrátane informácií, ako sú mená vývozcu, dovozcu, vydávajúcej banky a banky, v ktorej sa finančné prostriedky čerpajú.

V kontexte AML/CFT predstavuje zmenka jeden z klasických nástrojov obchodného financovania zneužívaných v rámci Trade-Based Money Laundering *(TBML)* – manipuláciou s hodnotou tovaru, falošným popisom zásielky alebo vystavovaním fiktívnych zmeniek bez reálneho obchodného základu možno efektívne presúvať hodnoty medzi jurisdikciami a zakrývať pôvod nelegálnych prostriedkov.

BILL OF LADING (NÁKLADNÝ LIST)

Požadovaný doklad, ktorý dopravca vydáva ako potvrdenie o prevzatí nákladu. Obsahuje druh a množstvo nákladu, ako aj miesto určenia.

V kontexte AML/CFT je nákladný list kľúčovým dokumentom pri odhaľovaní Trade-Based Money Laundering (TBML) – falšovanie alebo manipulácia s údajmi o druhu, množstve, hodnote alebo mieste určenia nákladu patrí medzi najrozšírenejšie techniky presunu nelegálnych hodnôt cez medzinárodný obchodný systém, pričom porovnávanie nákladného listu s ďalšími obchodnými dokumentmi (faktúra, colné vyhlásenie) je základným nástrojom odhalenia nezrovnalostí.

BILL STUFFING

Technika využívaná v kasínach, pri ktorej zákazník kasína vkladá hotovosť do výherných automatov s minimálnou alebo žiadnou skutočnou hernou aktivitou, zbiera výplatné lístky (TITO – ticket-in, ticket-out), a potom si peniaze nechá vyplatiť v pokladni kasína alebo požiada o šek.

V kontexte AML/CFT ide o klasickú techniku fázy umiestnenia (placement) v procese prania špinavých peňazí – kasíno je zneužité ako nástroj konverzie nelegálnej hotovosti na zdanlivo legitímne výhry, pričom výplatný šek z kasína poskytuje nelegálnym prostriedkom zdanie legálneho pôvodu; kasína sú preto v rámci AML/CFT považované za vysoko rizikové subjekty s povinnosťou zaviesť prísne kontrolné mechanizmy vrátane identifikácie hráčov, monitorovania transakcií a ohlasovania podozrivých aktivít.

BLACKLIST

Interný zoznam mien (vrátane miest, osôb, subjektov a jednotlivcov), ktoré sa preverujú s cieľom identifikovať prípadné vystavenie sankciám, ako aj zoznamy sankcií vedené vládou a dodávateľmi. Ďalšie potenciálne doplnenia interného čierneho zoznamu firmy môžu pochádzať z odporúčaní OFAC a iných varovaní, ktoré uvádzajú subjekty, ktoré sa síce nezaradili na zoznam SDN, ale stále sa považujú za vysoko rizikové. Čierna listina FATF je zoznam krajín, ktoré podľa rozhodnutia FATF nespolupracujú v medzinárodnom boji proti praniu špinavých peňazí a financovaniu terorizmu.

BLACK MARKET PESO EXCHANGE (BMPE)

Čierna burza s pesom (BMPE) je príkladom komplexnej metódy prania špinavých peňazí založenej na obchodovaní. Pôvodne bola BMPE poháňaná reštriktívnou politikou Kolumbie v oblasti výmeny mien. Aby tieto politiky obišli, kolumbijské podniky obchádzali vládne poplatky tým, že obchodovali so sprostredkovateľmi pesa, ktorí obchodovali na čiernom trhu alebo paralelnom finančnom trhu. Túto metódu využívali kolumbijskí

obchodníci s drogami, ktorí dostávali kolumbijské pesá v Kolumbii výmenou za americké doláre za drogy nachádzajúce sa v USA.

BLOCKADE

Nasadenie vojenských prostriedkov na zemi, vo vzduchu alebo na mori krajinou alebo koalíciou s cieľom zabrániť pohybu tovaru alebo osôb do cieľovej krajiny alebo z nej.

V kontexte AML/CFT je blokáda relevantná najmä zo sankčného hľadiska – krajina alebo región pod vojenskou blokádou je spravidla zároveň predmetom medzinárodných ekonomických sankcií, čo pre finančné inštitúcie znamená povinnosť dôsledného sankčného screeningu všetkých transakcií a obchodných vzťahov spojených s dotknutou jurisdikciou a zvýšenú ostražitosť voči pokusom o obchádzanie blokády prostredníctvom tretích krajín alebo fiktívnych obchodných štruktúr.

BOYCOTT

Odstúpenie od obchodnej alebo spoločenskej spolupráce alebo jej odmietnutie s vládou, organizáciou alebo jednotlivcom na znak protestu. V obchodnom kontexte sa bojkot používa ako synonymum pre exportné kontroly alebo embargá.

V kontexte AML/CFT je bojkot relevantný najmä v súvislosti so sankčným compliance – účasť na bojkote alebo naopak jeho obchádzanie môže mať priame právne dôsledky pre finančné inštitúcie; osobitne americká legislatíva (Export Administration Regulations) zakazuje americkým subjektom spolupracovať na bojkotoch, ktoré USA neuznávajú, a vyžaduje hlásenie žiadostí o účasť na takomto bojkote príslušným orgánom.

BUREAU OF INDUSTRY AND SECURITY (BIS)

Sekcia ministerstva obchodu USA zodpovedná za zabezpečenie správneho chápania, implementácie a presadzovania obchodných sankcií v USA. Okrem iných úloh BIS reguluje dovoz a vývoz citlivého tovaru a materiálov s dvojakým použitím a kontrolovaného tovaru a materiálov. Poslaním BIS je: „Podporovať národnú bezpečnosť, zahraničnú politiku a hospodárske ciele USA zabezpečením účinnej kontroly vývozu a systému dodržiavania zmlúv a podporou trvalého vedúceho postavenia USA v oblasti strategických technológií.“.

CARDHOLDER

Osoba, ktorej je vydaná platobná karta na vykonávanie finančných transakcií, alebo ďalšia osoba oprávnená používať kartu.

V kontexte AML/CFT je identifikácia skutočného držiteľa karty a osoby, ktorá kartu fakticky používa, kľúčovým prvkom KYC – zneužitie kariet tretími osobami, anonymné predplatené karty bez povinnej identifikácie a karty vydané na meno bábkových osôb *(straw man)* patria medzi bežné nástroje prania špinavých peňazí a obchádzania sankčných opatrení.

CARIBBEAN FINANCIAL ACTION TASK FORCE (CFATF)

Organizácia štátov a území karibskej oblasti, ktoré sa dohodli na vykonávaní spoločných opatrení proti praniu špinavých peňazí a financovaniu terorizmu. Zahŕňa karibské krajiny vrátane Aruby, Bahám, Britských Panenských ostrovov, Kajmanských ostrovov a Jamajky.

CASA DE CAMBIO (ZMENÁREŇ)

Casa de cambio, nazývaná aj „zmenáreň“ alebo „zmenáreň“, ponúka celý rad služieb, ktoré sú atraktívne pre subjekty zaoberajúce sa praním špinavých peňazí: výmenu valút a konsolidáciu bankoviek malých nominálnych hodnôt na väčšie, výmenu finančných nástrojov, ako sú cestovné šeky, peňažné poukážky a osobné šeky, a telegrafické prevody.

V kontexte AML/CFT patria zmenárne medzi vysoko rizikové subjekty s povinnosťou registrácie ako Money Services Business (MSB) a zavedenia plnohodnotného AML programu – kombinácia hotovostných transakcií, výmeny mien a prevodov bez potreby bankového účtu robí zo zmenární atraktívny nástroj pre fázu umiestnenia (placement) pri praní špinavých peňazí, štruktúrovanie platieb (smurfing), konverziu nelegálnej hotovosti do iných mien alebo finančných nástrojov a obchádzanie bankových kontrolných mechanizmov; osobitným rizikom sú neregistrované alebo nedostatočne regulované zmenárne pôsobiace v pohraničných oblastiach alebo v jurisdikciách s nízkymi štandardmi AML/CFT dohľadu.

CASH-INTENSIVE BUSINESS

Každý podnik, v ktorom zákazníci zvyčajne platia za poskytované produkty alebo služby v hotovosti, ako sú reštaurácie, donášková služba pizze, taxislužby, automaty na mince alebo autoumyvárne. Vysoký objem hotovostných transakcií je prirodzenou súčasťou ich obchodného modelu.

V kontexte AML/CFT predstavujú podniky s vysokým podielom hotovostných platieb jedno z najčastejšie zneužívaných prostredí na pranie špinavých peňazí, a to práve preto, že prirodzený tok hotovosti poskytuje ideálne krytie pre vmiešavanie nelegálnych prostriedkov do legitímnych tržieb – je prakticky nemožné overiť, či deklarované tržby skutočne pochádzajú z predaja produktov alebo služieb. Typickými varovnými signálmi sú tržby výrazne prevyšujúce priemer porovnateľných podnikov v danom sektore a lokalite, nezodpovedajúci počet zamestnancov alebo zákazníkov vzhľadom na deklarovaný obrat, pravidelné vklady hotovosti v okrúhlych sumách alebo tesne pod hranicou povinného hlásenia, absencia bežných obchodných výdavkov zodpovedajúcich deklarovanému obratu a neobvyklá geografická vzdialenosť medzi podnikom a bankou, kde sú vklady realizované. Finančné inštitúcie sú povinné pri klientoch prevádzkujúcich cash-intensive businesses uplatňovať zvýšenú hĺbkovú previerku, pravidelne porovnávať deklarované tržby s transakčnou aktivitou na účte a pri odchýlkach od očakávaného vzorca zvážiť podanie oznámenia o podozrivej aktivite.

CASH COLLATERALIZED LOANS

Úver zabezpečený hotovosťou má ako zábezpeku úveru hotovostné vklady. Hotovostné vklady sa niekedy môžu nachádzať aj v inej jurisdikcii.

V kontexte AML/CFT patria úvery zabezpečené hotovostným kolaterálom k klasickým technikám prania špinavých peňazí – páchateľ uloží nelegálne získanú hotovosť ako kolaterál (často v offshore jurisdikcii), získa legitímny úver v inej jurisdikcii, úver následne spláca z tých istých nelegálnych prostriedkov a výsledkom je zdanlivo legálny príjem z úveru; táto technika efektívne preruší sledovateľnosť pôvodu prostriedkov a je preto predmetom zvýšenej pozornosti pri hĺbkovej previerke klientov žiadajúcich o úvery s neštandardnou štruktúrou kolaterálu.

CASH DEPOSITS

Sumy peňazí uložené na jednom alebo viacerých účtoch vo finančnej inštitúcii. Hotovostné vklady sú prirodzenou a bežnou súčasťou finančného systému pre fyzické aj právnické osoby.

V kontexte AML/CFT predstavujú hotovostné vklady najzraniteľnejší bod celého finančného systému – ide o klasický nástroj fázy umiestnenia (placement), teda prvého a najrizikovejšieho kroku v procese prania špinavých peňazí, keď sa páchatelia snažia dostať nelegálnu hotovosť do bezhotovostnej ekonomiky. Práve preto väčšina jurisdikcií stanovuje povinnosť hlásiť hotovostné transakcie nad určitú hranicu (v USA napríklad 10 000 USD podľa Bank Secrecy Act, v EÚ sa limity líšia podľa členského štátu), pričom páchatelia na obchádzanie týchto limitov systematicky využívajú techniku štruktúrovania *(structuring alebo smurfing)* – rozkladajú väčšie sumy na sériu menších vkladov pod hranicou povinného hlásenia,

realizovaných na rôznych pobočkách, v rôznych časoch alebo prostredníctvom rôznych osôb. Finančné inštitúcie sú povinné monitorovať nielen jednotlivé vklady prekračujúce stanovené limity, ale aj vzorce správania naznačujúce štruktúrovanie, neobvyklú frekvenciu vkladov, vklady nezodpovedajúce deklarovanému profilu klienta alebo vklady realizované v geograficky vzdialených pobočkách bez zjavného dôvodu.

CASHIER'S CHECK

Bežný peňažný nástroj vystavený priamo finančnou inštitúciou na vlastný účet, ktorý predstavuje jej priamy záväzok voči príjemcovi. Na rozdiel od osobného šeku je platba garantované samotnou bankou, čo z neho robí široko akceptovaný platobný prostriedok pri významnejších transakciách.

V kontexte AML/CFT predstavuje bankový šek rizikový nástroj práve preto, že konvertuje hotovosť na legitímne vyzerajúci bankový nástroj – páchateľ nakúpi za nelegálnu hotovosť bankový šek, čím preruší priamu väzbu medzi hotovosťou a jej nelegálnym pôvodom; šek vystavený na meno banky následne pôsobí ako dôveryhodný doklad o legálnom pôvode prostriedkov. Typickými varovnými signálmi sú nákup viacerých šekov v hodnotách tesne pod hranicou povinného hlásenia, nákup šekov za hotovosť osobami bez existujúceho vzťahu s bankou, šeky vystavené na tretie osoby bez zjavného obchodného dôvodu a následný rýchly vklad alebo výmena šeku v inej inštitúcii alebo jurisdikcii.

CENTRAL BANK DIGITAL CURRENCY (CBDC)

Digitálna forma fiat meny emitovaná a garantovaná centrálnou bankou. Na rozdiel od kryptomien je CBDC centralizovaná a priamo záväzková pre centrálnu banku. Z pohľadu AML/CFT prináša CBDC nové príležitosti (sledovateľnosť transakcií) aj výzvy (ochrana súkromia, cezhraničné toky). FATF monitoruje vývoj CBDC s ohľadom na riziká prania špinavých peňazí.

COMISIÓN INTERAMERICANA PARA EL CONTROL DEL ABUSO DE DROGAS OR INTER-AMERICAN DRUG ABUSE CONTROL COMMISSION (CICAD)

Je konzultačným a poradným orgánom OAS[3] v oblasti drog. Slúži ako fórum pre členské štáty OAS na diskusiu a hľadanie riešení drogovej problematiky a poskytuje im technickú pomoc na zvýšenie ich kapacity v boji proti drogovej problematike. Od svojho založenia v roku 1986 CICAD a jeho výkonný sekretariát reagujú na neustále sa meniace výzvy v oblasti kontroly drog a rozširujú svoje úsilie o podporu regionálnej spolupráce a koordinácie s členskými štátmi a medzi nimi. Polosférická protidrogová stratégia OAS, prijatá v roku 2010, pristupuje k svetovému problému drog ako ku komplexnému, dynamickému a multipríčinnému javu, ktorý si vyžaduje komplexný, vyvážený a multidisciplinárny prístup. Stratégia uznáva drogovú závislosť ako ochorenie, ktoré by sa malo riešiť ako otázka verejného zdravia, a vyzýva krajiny, aby zachovali primeranú rovnováhu medzi aktivitami zameranými na znižovanie dopytu a znižovanie ponuky. Polosférický akčný plán boja proti drogám (2016 - 2020), ktorý je sprievodcom implementácie stratégie, stanovuje prioritné opatrenia pre členské štáty OAS, pričom do centra protidrogovej politiky kladie jednotlivcov a zahŕňa prierezovú perspektívu ľudských práv, rodovej rovnosti a rozvoja so zameraním na protidrogové politiky založené na dôkazoch. Prostredníctvom svojho ročného programovania a širokej škály národných a regionálnych projektov na pologuli pomáha CICAD členským štátom pri posilňovaní ich protidrogových politík vykonávaním hĺbkového výskumu a hodnotenia týkajúceho sa drogových otázok a nových trendov a poskytovaním účinnej technickej pomoci a špecializovanej odbornej prípravy zameranej na budovanie kapacít. CICAD úzko spolupracuje s partnermi, ako sú Úrad OSN pre drogy a kriminalitu, Medzinárodný výbor pre kontrolu drog, Panamerická zdravotnícka organizácia, Karibské spoločenstvo (CARICOM), Európske monitorovacie centrum pre drogy a drogovú závislosť a Regionálny bezpečnostný systém. CICAD tiež udržiava silné väzby s občianskou spoločnosťou vrátane účasti občianskej spoločnosti na všetkých pravidelných zasadnutiach CICAD.

COLLECTION ACCOUNTS

Účty, na ktoré viacero osôb ukladá malé sumy, ktoré sa následne konsolidujú a prevádzajú na účet v inej – spravidla zahraničnej – jurisdikcii, pričom pôvod jednotlivých vkladov nie je zdokumentovaný.

V kontexte AML/CFT predstavujú zberné účty typologický vzorec spájajúci niekoľko rizikových prvkov súčasne – agregáciu hotovostných vkladov od viacerých prispievateľov, cezhraničný prevod konsolidovaných prostriedkov a absenciu dokumentácie o pôvode finančných prostriedkov. Tieto účty môžu byť zneužité na pranie špinavých peňazí, obchádzanie požiadaviek na hlásenie hotovostných transakcií a na neformálne remitancie mimo regulovaného systému prevodu hodnôt. Je pritom dôležité zdôrazniť, že zberné účty využívané migrantmi na zasielanie legitímnych remitancií do domovských krajín sú bežnou a legálnou praxou – AML/CFT riziko nevyplýva z etnického pôvodu používateľov, ale výlučne z absencie dokumentácie o pôvode prostriedkov, štruktúry transakcií a neobvyklých vzorcov správania na účte. Finančné inštitúcie sú povinné posudzovať riziko na základe objektívnych transakčných charakteristík, nie na základe národnosti alebo etnicity klientov, a pri identifikácii zberných účtov bez dostatočnej dokumentácie zdrojov prostriedkov uplatniť zvýšenú hĺbkovú previerku a zvážiť podanie oznámenia o podozrivej aktivite.

COMMISSION ROGATOIRE

Rogačná komisia, známa aj ako súdny príkaz, je písomná žiadosť o právnu alebo súdnu pomoc, ktorú ústredný orgán jednej krajiny zasiela ústrednému orgánu inej krajiny, keď žiada o dôkazy od zahraničnej jurisdikcie. V liste sa zvyčajne uvádza povaha žiadosti, príslušné trestné obvinenia v dožadujúcej krajine, právne ustanovenie, na základe ktorého sa žiadosť podáva, a požadované informácie.

COMPETENT AUTHORITIES

Príslušnými orgánmi sa rozumejú všetky orgány verejnej moci[4], ktoré sú zodpovedné za boj proti praniu špinavých peňazí a/alebo financovaniu terorizmu. Patria sem najmä FIU; orgány, ktoré majú funkciu vyšetrovania a/alebo stíhania prania špinavých peňazí, súvisiacich predikatívnych trestných činov a financovania terorizmu a zaistenia/zamrazenia a konfiškácie majetku pochádzajúceho z trestnej činnosti; orgány, ktoré prijímajú správy o cezhraničnej preprave peňazí a BNI; a orgány, ktoré majú povinnosti v oblasti dohľadu alebo monitorovania AML/CFT zamerané na zabezpečenie dodržiavania požiadaviek AML/CFT zo strany finančných inštitúcií a DNFBP. SRB sa nemajú považovať za príslušné orgány.

COMPLIANCE

Činnosť alebo stav dodržiavania súboru právnych predpisov, nariadení, pravidiel, politiky, špecifikácií alebo chápaných noriem.

V kontexte AML/CFT má compliance oveľa širší a aktívnejší rozmer než len pasívne dodržiavanie predpisov – nejde o jednorazový stav, ale o kontinuálny proces, ktorý zahŕňa identifikáciu a hodnotenie relevantných AML/CFT povinností vyplývajúcich z národnej legislatívy, medzinárodných

[3] Organizácia amerických štátov (OAS) je najstaršou regionálnou organizáciou na svete, ktorej vznik sa datuje od prvej medzinárodnej konferencie amerických štátov, ktorá sa konala vo Washingtone od októbra 1889 do apríla 1890. Na tomto zasadnutí bolo schválené založenie Medzinárodnej únie amerických republík a pripravila sa pôda na utkanie siete ustanovení a inštitúcií, ktoré sa stali známe ako medziamerický systém, najstarší medzinárodný inštitucionálny systém.

[4] Patria sem aj orgány finančného dohľadu zriadené ako nezávislé mimovládne orgány so zákonnými právomocami.

štandardov (FATF, smernice AMLD) a interných politík, zavedenie a udržiavanie účinného AML programu primeraného rizikovému profilu inštitúcie, priebežné monitorovanie jeho funkčnosti a aktualizáciu v reakcii na meniace sa regulačné požiadavky a nové typológie. Zodpovednosť za AML/CFT compliance nesie celá inštitúcia v rámci modelu troch línií obrany – prvá línia (obchodné jednotky) ako primárny nositeľ rizika, druhá línia (compliance funkcia a MLRO) ako kontrolný a poradenský orgán a tretia línia (interný audit) ako nezávislý overovateľ účinnosti celého systému. Regulátori pritom dôsledne rozlišujú medzi formálnym súladom – teda existenciou dokumentov a procesov na papieri – a skutočným súladom, ktorý sa prejavuje funkčnosťou kontrol v praxi; práve tento rozdiel je predmetom dohľadových inšpekcií a hodnotení, pričom formálny súlad bez skutočnej účinnosti nie je pre regulátora akceptovateľný.

CONCENTRATION ACCOUNT

Nazýva sa tiež „súhrnný účet". Zúčtovací účet vedený finančnou inštitúciou v jej mene sa používa najmä na interné administratívne transakcie alebo transakcie medzi bankami, pri ktorých sa finančné prostriedky prenášajú a kombinujú bez osobnej identifikácie pôvodcov.

V kontexte AML/CFT predstavujú koncentračné účty jedno z najvýznamnejších vnútorných rizík finančnej inštitúcie, keďže agregácia prostriedkov od viacerých klientov na jednom účte efektívne prerušuje auditovateľnú stopu (audit trail) medzi konkrétnym klientom a jeho transakciami – čo je presne ten efekt, ktorý páchatelia prania špinavých peňazí aktívne hľadajú. Regulátori, vrátane FinCEN v USA a orgánov dohľadu v EÚ, preto vyžadujú, aby finančné inštitúcie zaviedli prísne vnútorné kontroly pri používaní koncentračných účtov: každá transakcia prechádzajúca koncentračným účtom musí byť spätne priraditeľná ku konkrétnemu klientovi a jeho účtu, klienti nesmú byť informovaní o čísle koncentračného účtu inštitúcie ani ho nesmú využívať na priame vklady, systémy monitorovania transakcií musia byť schopné sledovať pohyby prostriedkov aj napriek ich zlučovaniu a zamestnanci pracujúci s koncentračnými účtami musia byť osobitne vyškolení na rozpoznávanie varovných signálov ich zneužitia. Porušenie týchto zásad patrí medzi najčastejšie nedostatky identifikované pri dohľadových inšpekciách zameraných na AML/CFT.

CONCENTRATION RISK

Riziko vyplývajúce z nadmernej angažovanosti voči jednému subjektu, skupine spriaznených subjektov, sektoru, geografickej oblasti alebo typu produktu. Na strane aktív súvahy regulátori vyžadujú od finančných inštitúcií zavedenie informačného systému na identifikáciu úverových koncentrácií a stanovenie limitov angažovanosti voči jednotlivým dlžníkom alebo skupinám spriaznených dlžníkov. Na strane pasív je riziko koncentrácie spojené s rizikom financovania – predčasný a náhly výber prostriedkov veľkými vkladateľmi môže vážne ohroziť likviditu inštitúcie.

V kontexte AML/CFT má riziko koncentrácie osobitnú dimenziu, ktorá presahuje tradičné prudenciálne chápanie – vysoká koncentrácia klientov, transakcií alebo príjmov z konkrétneho sektora, geografickej oblasti alebo typu produktu so zvýšeným rizikovým profilom priamo zvyšuje celkové AML/CFT riziko inštitúcie. Príkladom je nadmerná koncentrácia klientov z vysoko rizikových jurisdikcií, koncentrácia v sektoroch náchylných na pranie špinavých peňazí (nehnuteľnosti, kasína, obchodníci s drahými kovmi) alebo závislosť na obmedzenom počte korešpondenčných bánk so slabým AML/CFT rámcom. Regulátori preto očakávajú, že hodnotenie rizika koncentrácie bude integrálnou súčasťou celkového AML/CFT hodnotenia rizík inštitúcie a že existencia významných koncentrácií v rizikových segmentoch bude zohľadnená pri nastavení kontrol, limitov a intenzity monitorovania.

CONFIDENTIALITY

Udržiavanie určitých skutočností, údajov a informácií mimo dosahu verejnosti alebo neoprávnených osôb. V kontexte finančných inštitúcií ide o zásadnú právnu povinnosť vyplývajúcu z predpisov o bankovom tajomstve, ochrane osobných údajov a profesijnej mlčanlivosti.

V kontexte AML/CFT vytvára povinnosť dôvernosti jedinečné a navzájom protichodné napätie, ktoré nemá v iných oblastiach compliance obdobu. Na jednej strane povinnosť zachovávať mlčanlivosť voči klientovi je absolútna v súvislosti s podaným oznámením o podozrivej aktivite *(SAR/STR)* – zamestnanci finančnej inštitúcie sú pod hrozbou trestnej sankcie zakázaní informovať klienta alebo akúkoľvek tretiu osobu o tom, že bolo podané hlásenie alebo že prebieha vyšetrovanie; tento zákaz je známy ako zákaz tipping off a jeho porušenie môže zmariť prebiehajúce vyšetrovanie. Na druhej strane tá istá povinnosť dôvernosti, ktorá chráni klientov pred neoprávneným zdieľaním ich informácií, môže byť v niektorých jurisdikciách zneužívaná ako nástroj na blokovanie oprávnenej výmeny informácií medzi finančnými inštitúciami a orgánmi činnými v trestnom konaní alebo finančnými spravodajskými jednotkami – práve preto moderná AML/CFT legislatíva explicitne stanovuje výnimky z bankového tajomstva pre účely AML/CFT a zabezpečuje právnu ochranu (safe harbor) pre inštitúcie, ktoré v dobrej viere podajú oznámenie o podozrivej aktivite, aj keby sa neskôr ukázalo, že podozrenie nebolo opodstatnené. Rovnako dôležitá je otázka zdieľania informácií medzi finančnými inštitúciami v rámci skupiny alebo medzi nespojenými inštitúciami – väčšina jurisdikcií toto zdieľanie za presne stanovených podmienok umožňuje práve s cieľom zvýšiť účinnosť boja proti praniu špinavých peňazí, pričom hranica medzi povoleným zdieľaním a porušením dôvernosti musí byť starostlivo dodržiavaná.

CONFISCATION

Znamená trvalé odňatie finančných prostriedkov alebo iného majetku na základe rozhodnutia príslušného orgánu alebo súdu. Konfiškácia alebo prepadnutie sa uskutočňuje prostredníctvom súdneho alebo správneho konania, ktorým sa vlastníctvo určených finančných prostriedkov alebo iného majetku prevádza na štát. Po prevode stráca osoba (osoby) alebo subjekt (subjekty), ktoré mali v čase konfiškácie alebo prepadnutia podiel na určených finančných prostriedkoch alebo inom majetku, v zásade všetky práva na skonfiškovaný alebo prepadnutý majetok. Príkazy na konfiškáciu alebo prepadnutie sú zvyčajne spojené s odsúdením za trestný čin alebo so súdnym rozhodnutím, ktorým sa určilo, že skonfiškovaný alebo prepadnutý majetok pochádza z porušenia zákona alebo bol určený na jeho použitie k porušeniu zákona.

CONSOLIDATION OF GOODS

Metóda vyhýbania sa sankciám alebo exportným kontrolným opatreniam, pri ktorej osoba alebo organizácia buď zoskupí malé zásielky do jednej väčšej zásielky, alebo zmieša obmedzené položky s iným tovarom a nedeklaruje tieto obmedzené položky v prepravnej dokumentácii.

V kontexte AML/CFT a sankčného compliance predstavuje konsolidácia tovaru typickú techniku využívanú pri obchádzaní exportných kontrol, sankčných režimov a v rámci Trade-Based Money Laundering (TBML) – zmiesením kontrolovaného alebo sankcionovaného tovaru s legálnym nákladom a jeho nedeklarovaním v sprievodnej dokumentácii páchatelia efektívne zakrývajú skutočný obsah zásielky, obchádzajú colné kontroly a umožňujú transfer zakázaného tovaru alebo hodnôt do cieľových jurisdikcií; finančné inštitúcie financujúce medzinárodný obchod sú preto povinné venovať zvýšenú pozornosť prípadom, keď popis tovaru v platobných dokumentoch nezodpovedá fyzickej povahe zásielky, keď trasy prepravy nie sú ekonomicky odôvodnené alebo keď transakcie zahŕňajú jurisdikcie alebo protistrany so sankčným rizikom.

CONTROL EFFECTIVENESS

Meranie kvality a funkčnosti kontrolných mechanizmov zavedených na zmiernenie identifikovaných rizík. Tieto kontrolné mechanizmy by mali byť

nielen vhodné, ale zároveň aj účinné v praxi, čo znamená, že musia byť primerané povahe a úrovni rizika, ktoré majú zmierňovať. Pri zvýšenom rizikovom profile sú nevyhnutné komplexnejšie a prísnejšie kontrolné mechanizmy.

V kontexte AML/CFT je účinnosť kontrolných mechanizmov jedným z ústredných pojmov moderného prístupu založeného na riziku – regulátori a hodnotitelia FATF pri vzájomných hodnoteniach krajín explicitne rozlišujú medzi technickým súladom (existencia predpisov a postupov na papieri) a skutočnou účinnosťou (reálne fungovanie systému v praxi). Práve tento rozdiel je jadrom metodológie FATF: krajina môže formálne spĺňať všetky požiadavky, ale ak jej kontrolné mechanizmy nie sú účinné, hodnotenie bude negatívne. Rovnaký princíp uplatňujú regulátori pri dohľade nad finančnými inštitúciami – nestačí mať zavedené politiky a postupy, ale je nevyhnutné pravidelne testovať a preukazovať ich skutočnú funkčnosť prostredníctvom interného auditu, back-testingu monitorovacích pravidiel, pravidelného prehodnocovania prahových hodnôt a vyhodnocovania kvality podaných oznámení o podozrivých aktivitách. Nízka účinnosť kontrolných mechanizmov napriek ich formálnej existencii je pre regulátorov signálom systémového zlyhania compliance funkcie a môže viesť k regulačným opatreniam, pokutám alebo iným sankciám voči inštitúcii.

CORE PRINCIPLES (CPS)

Základné zásady účinného bankového dohľadu (Core principles for effective banking supervision - CPs) predstavujú minimálne globálne štandardy pre spoľahlivú prudenciálnu reguláciu a dohľad nad bankami. Pôvodne boli zverejnené v roku 1997 a aktualizované v rokoch 2006 a 2012 a obsahujú 29 zásad. Všetky sú univerzálne použiteľné, a to aj preto, že CPs obsahujú koncepciu proporcionality, čím sa prispôsobujú rôznym bankovým systémom a širokému spektru bánk (od veľkých medzinárodne pôsobiacich bánk až po malé inštitúcie prijímajúce vklady). Orgány dohľadu využívajú CPs ako referenčnú hodnotu na hodnotenie kvality svojich regulačných a dohľadových rámcov a na pomoc pri určovaní budúcich pracovných priorít. Využívajú ich aj Medzinárodný menový fond a Svetová banka na hodnotenie účinnosti systémov bankového dohľadu krajín v rámci svojho programu hodnotenia finančného sektora. V tomto zhrnutí sa uvádzajú predpoklady potrebné na účinný dohľad a 29 CPs, ktoré sa považujú za nevyhnutné na podporu spoľahlivého systému dohľadu.

CORPORATE VEHICLES

Typy právnických osôb, ktoré môžu byť predmetom zneužitia, ako sú spoločnosti s ručením obmedzeným alebo akciové spoločnosti, s ktorých akciami sa neobchoduje na burze cenných papierov, trusty, neziskové organizácie, komanditné spoločnosti a spoločnosti s ručením obmedzeným a súkromné investičné spoločnosti. Niekedy je ťažké identifikovať osoby, ktoré sú konečnými skutočnými vlastníkmi alebo kontrolórmi právnických osôb *(Ultimate Beneficial Owner - UBO)*, čo spôsobuje, že tieto subjekty sú zraniteľné voči praniu špinavých peňazí.

CORRESPONDENT BANKING

Poskytovanie bankových služieb jednou bankou (korešpondenčná banka), inej banke (respondentská banka). Veľké medzinárodné banky zvyčajne pôsobia ako korešpondenti pre stovky iných bánk na celom svete. Respondentským bankám môžu poskytovať širokú škálu služieb vrátane správy hotovosti (napr. úročené účty v rôznych menách), medzinárodných bankových prevodov finančných prostriedkov, služieb zúčtovania šekov, priebežných účtov a devízových služieb.

COUNTER TERRORIST ACTION GROUP (CTAG)

Akčná skupina pre boj proti terorizmu (CTAG), ktorú zriadila skupina G8, má za cieľ podporovať Výbor Bezpečnostnej rady OSN pre boj proti terorizmu, a to predovšetkým prostredníctvom koordinácie a osvetovej činnosti. Skupina CTAG sa napríklad snaží koordinovať príspevky na činnosti súvisiace s budovaním kapacít v oblasti boja proti terorizmu, napríklad v súvislosti s odbornou prípravou, financovaním, odbornými znalosťami a vybavením, ako aj technickou a právnou pomocou iným krajinám. S cieľom zabrániť duplicite úsilia si skupina CTAG vymieňa aj osvedčené postupy a získané skúsenosti. Členmi CTAG sú členovia skupiny G8 (vedúci predstavitelia Kanady, Francúzska, Nemecka, Talianska, Japonska, Ruska, Spojeného kráľovstva a Spojených štátov amerických).

COUNTER-TERRORISM FINANCING (CTF/CFT)

CTF/CFT znamená právne predpisy a politiky prijaté krajinami na odhaľovanie, vyšetrovanie a nahlasovanie akýchkoľvek činností, ktoré vedú k financovaniu teroristických aktivít, ako je nábor teroristov, udržiavanie logistiky alebo vykonávanie teroristických operácií. Skratka AML/CTF sa objavuje najmä v austrálskej a ázijsko-tichomorskej legislatíve, v rámci FATF, EÚ a medzinárodného štandardu je zaužívaná forma AML/CFT.

COUNTER-TERRORISM COMMITTEE (CTC)

CTC pracuje na posilnení schopnosti členských štátov OSN predchádzať teroristickým činom v rámci svojich hraníc, ako aj medzi regiónmi. CTC v jeho úsilí pomáha Výkonné riaditeľstvo Protiteroristického výboru (CTED), ktoré vykonáva politické rozhodnutia výboru, vykonáva odborné hodnotenia jednotlivých členských štátov a sprostredkúva krajinám technickú pomoc v oblasti boja proti terorizmu.

CREDIT CARD

Plastová karta s úverovým limitom, ktorá sa používa na nákup tovaru a služieb a na získanie hotovostných záloh na úver. Vydavateľ následne vystaví držiteľovi karty faktúru na splatenie poskytnutého úveru. Kreditné karty sa môžu používať na pranie špinavých peňazí, keď sa platby dlžných súm na karte vykonávajú z peňazí pochádzajúcich z trestnej činnosti.

CRIMINAL PROCEEDS

Akýkoľvek majetok pochádzajúci alebo získaný priamo alebo nepriamo spáchaním trestného činu.

CROSS-BORDER

Používa sa v súvislosti s činnosťami, ktoré zahŕňajú aspoň dve krajiny, napríklad prevod peňazí z jednej krajiny do druhej alebo prepravu meny cez hranice.

CURRENCY

Bankovky a mince, ktoré sú v obehu ako prostriedok výmeny.

V kontexte AML/CFT predstavuje hotovosť najvyššie rizikový platobný prostriedok v celom finančnom systéme, a to práve pre svoje inherentné vlastnosti – anonymitu, okamžitú dostupnosť, jednoduchosť prenosu a praktickú nesledovateľnosť. Hotovosť je ústredným nástrojom fázy umiestnenia (placement) v procese prania špinavých peňazí a väčšina AML/CFT regulačných povinností – oznamovanie hotovostných transakcií nad stanovené limity, zákaz platby v hotovosti nad určitú sumu, povinná identifikácia pri hotovostných transakciách – je priamo zameraná na kontrolu hotovostných tokov. Osobitnou výzvou posledných rokov je postupné rozširovanie pojmu „mena“ v regulačnom kontexte – FATF a národní regulátori čoraz viac pracujú s konceptom virtuálnych aktív ako digitálnej obdoby hotovosti, ktoré prinášajú podobné anonymizačné riziká ako fyzická hotovosť, avšak v celosvetovom meradle a s oveľa väčšou rýchlosťou pohybu hodnôt.

CURRENCY SMUGGLING

Nezákonný pohyb veľkého množstva hotovosti cez hranice, často do krajín bez prísneho bankového tajomstva, slabej devízovej kontroly alebo nedostatočných právnych predpisov proti praniu špinavých peňazí.

CURRENCY TRANSACTION REPORT (CTR)

Správa, ktorá dokumentuje fyzickú menovú transakciu, ktorá presahuje určitú peňažnú hranicu. CTR je možné podať aj pri viacerých menových transakciách, ktoré sa uskutočnia v jeden deň a prekročia požadovanú sumu na vykazovanie. Niektoré krajiny vrátane USA majú požiadavky, ktoré riešia, kedy sa má CTR podať štátnym orgánom.

CUSTODIAN

Banka, finančná inštitúcia alebo iný subjekt, ktorý je zodpovedný za riadenie, správu alebo úschovu aktív pre iné osoby alebo inštitúcie. Správca drží aktíva s cieľom minimalizovať riziko krádeže alebo straty a aktívne s nimi neobchoduje ani s nimi nenakladá.

CUSTODY

Činnosť alebo právomoc chrániť a spravovať investície alebo majetok klientov, zvyčajne vykonávaná regulovaným subjektom – bankou, obchodníkom s cennými papiermi alebo špecializovanou inštitúciou *(Custodian)*.

V kontexte AML/CFT predstavuje poskytovanie custodian služieb špecifické riziko, keďže inštitúcia spravuje majetok, ktorého skutočný vlastník a pôvod nemusia byť transparentné – povinnosť identifikácie skutočného vlastníka (beneficial owner) spravovaného majetku, overenia pôvodu aktív zverených do úschovy a priebežného monitorovania pohybov s týmto majetkom patrí medzi kľúčové AML/CFT povinnosti custodian inštitúcií, pričom osobitne rizikové sú situácie, keď je majetok zverený do správy prostredníctvom zložitých právnych štruktúr (trusty, nadácie, holdingové spoločnosti) navrhnutých tak, aby zatajili totožnosť skutočného vlastníka.

CUSTOMER DUE DILIGENCE (CDD)

Súbor vnútorných kontrolných mechanizmov, ktoré finančnej inštitúcii umožňujú zistiť totožnosť klienta, s relatívnou istotou predvídať typy transakcií, do ktorých sa klient pravdepodobne zapojí, a posúdiť, do akej miery ju klient vystavuje rôznym rizikám (t. j. praniu špinavých peňazí a sankciám). Organizácie tiež potrebujú poznať svojich klientov prostredníctvom CDD, aby sa chránili pred podvodmi a dodržiavali požiadavky príslušných právnych predpisov a nariadení. Účinné programy CDD pomáhajú chrániť aj dobré meno bánk a integritu bankových systémov tým, že znižujú pravdepodobnosť, že sa banky stanú nástrojom alebo obeťou finančnej trestnej činnosti. Ako také predstavujú dôležitú súčasť riadneho riadenia rizík.

CUSTOMER RELATIONSHIP

Vzťah so zákazníkom zahŕňa akýkoľvek kontakt s potenciálnym zákazníkom. Patrí sem dialóg, ktorý sa uskutočňuje počas nástupu, a rozhovory, ku ktorým dochádza, keď zákazník využíva produkty a služby finančnej inštitúcie. Na tejto komunikácii sa môžu podieľať ľudia z manažmentu, marketingu, prevádzkových oddelení a oddelení pre dodržiavanie predpisov finančnej inštitúcie.

CUSTOMER RISK RATING / RISK SCORING

Hodnotenie úrovne rizika prania špinavých peňazí spojeného s konkrétnym zákazníkom na základe rôznych faktorov, ako sú geografia, typ zákazníka, produkty, služby, kanály doručenia a správanie pri transakciách. Výsledné hodnotenie rizika určuje rozsah opatrení hĺbkovej previerky zákazníka (CDD/EDD/SDD) a frekvenciu monitorovania.

V kontexte AML/CFT je hodnotenie rizika zákazníka základným pilierom prístupu založeného na riziku (risk-based approach) vyžadovaného FATF a smerniciami AMLD – namiesto jednotného zaobchádzania so všetkými klientmi umožňuje inštitúciám koncentrovať zdroje a kontrolné mechanizmy tam, kde je riziko najvyššie. Kvalita a spoľahlivosť rizikového hodnotenia pritom priamo ovplyvňuje celkovú účinnosť AML/CFT programu inštitúcie. Regulátori pri dohľadových inšpekciách osobitne skúmajú metodológiu rizikového skóringu – či sú použité faktory relevantné a dostatočne granulárne, či model skutočne odráža reálne riziko alebo len formálne plní regulačné požiadavky, či sú rizikové hodnotenia pravidelne aktualizované pri zmene okolností a či existuje mechanizmus manuálneho prehodnotenia automaticky priradeného skóre. Osobitnou výzvou je dynamická povaha rizika – hodnotenie pridelené pri otvorení účtu sa môže v čase výrazne zmeniť v dôsledku zmien v správaní klienta, jeho vlastníckej štruktúre, obchodných aktivitách alebo v dôsledku nových typológií identifikovaných regulátormi, čo si vyžaduje systém priebežného prehodnocovania spúšťaného konkrétnymi udalosťami (trigger-based review) aj pravidelného periodického prehodnocovania celého klientského portfólia.

DE-RISKING

Prax finančných inštitúcií spočívajúca v ukončení alebo obmedzení obchodných vzťahov s kategóriami zákazníkov, produktov alebo geografickými oblasťami s vnímaným vyšším rizikom AML/CFT bez posúdenia individuálneho rizika. FATF a medzinárodné orgány de-risking neodporúčajú, pretože môže viesť k finančnému vylúčeniu a presunu transakcií do neregulovaných kanálov.

DEALING IN FUNDS

Prax spočívajúca v tom, že finančná inštitúcia presúva, prevádza, mení, používa alebo sprístupňuje finančné prostriedky, ktoré zmrazila. Nakladanie s finančnými prostriedkami zahŕňa aj akúkoľvek interakciu s finančnými prostriedkami, ktorá by viedla k akejkoľvek zmene ich objemu, výšky, umiestnenia, vlastníctva, držby, charakteru alebo určenia, alebo k akejkoľvek zmene, ktorá by umožnila použitie finančných prostriedkov, vrátane správy portfólia. Obmedzenia týkajúce sa zmrazenia aktív vyžadujú, aby boli zmrazené aktíva oddelené.

DEBIT CARD

Karta, ktorá umožňuje držiteľovi účtu čerpať finančné prostriedky z existujúceho účtu. Debetné karty sa používajú na úhradu záväzkov alebo nákupov. Debetné karty možno používať na rôznych miestach vrátane internetu. Debetné karty často umožňujú pohyb hotovosti prostredníctvom transakcií s vrátením hotovosti alebo výberov v bankomatoch.

DECISION TREE

Metóda hodnotenia rizika prania špinavých peňazí založená na rozhodovacom strome - postupu otázok na určenie toho, ktoré upozornenia (alerts) možno odôvodnene vylúčiť a ktoré si vyžadujú prešetrenie.

V kontexte AML/CFT je rozhodovací strom praktickým nástrojom štandardizácie a dokumentácie procesu vyhodnocovania alertov v rámci transaction monitoringu – zabezpečuje, že analytici postupujú konzistentne, ich rozhodnutia sú odôvodnené a auditovateľné a že žiadny relevantný faktor nie je prehliadnutý. Regulátori pri dohľadových inšpekciách kladú dôraz nielen na existenciu rozhodovacieho stromu, ale aj na jeho kvalitu a primeranosť – príliš jednoduchý alebo rigidný rozhodovací strom môže viesť k mechanickému uzatváraniu alertov bez skutočného posúdenia rizika, čo predstavuje systémové zlyhanie monitorovacieho procesu; naopak, dobre navrhnutý rozhodovací strom zohľadňuje rizikový profil klienta, históriu transakcií, aktuálne typológie a kontext konkrétnej transakcie, čím zvyšuje kvalitu výsledných rozhodnutí a znižuje podiel falošne pozitívnych výsledkov bez ohrozenia schopnosti identifikovať skutočné podozrivé aktivity.

DELISTING

Proces odstránenia cieľa/subjektu/objektu sankcií zo zoznamu po zrušení obmedzení, ktoré naň boli uvalené.

DELIVERY CHANNEL

Spôsoby, akými firma poskytuje produkty a služby svojim zákazníkom (označované aj ako spôsoby obsluhy a distribučné kanály). Napríklad spoliehanie sa na maklérov, sprostredkovateľov a iné nezávislé tretie strany predstavuje vyššie sankčné riziko, ako keď podnik komunikuje priamo so zákazníkmi a dodávateľmi. Absencia osobného kontaktovania predstavuje vyššie riziko, ako keď sú zákazníci kontaktovaní priamo alebo prostredníctvom domácej pobočky. Iné dodávateľské kanály bez osobného kontaktu, ako napríklad internetové bankovníctvo a podniky poskytujúce peňažné služby, sa tiež považujú za subjekty, ktoré predstavujú vyššie inherentné sankčné riziko. Vyššie riziko predstavuje aj doručovací kanál, ktorý rýchlo spracúva platby.

DENIED PERSONS LIST (DPL)

Zoznam osôb, subjektov alebo spoločností, ktorým boli zamietnuté vývozné privilégiá, najčastejšie z dôvodu porušenia zákona o správe vývozu, ktorý zverejňuje BIS. Americkým spoločnostiam a jednotlivcom sa zakazuje vstupovať do akýchkoľvek vývozných transakcií s akoukoľvek osobou alebo subjektom uvedeným na zozname DPL.

DESIGNATED CATEGORIES OF OFFENSE

Trestné činy, ktoré FATF považuje za predikatívne trestné činy prania špinavých peňazí. Každá krajina sa môže samostatne rozhodnúť, ako bude definovať konkrétne trestné činy a ich prvky podľa svojich vnútroštátnych právnych predpisov. Mnohé krajiny nešpecifikujú, ktoré trestné činy môžu slúžiť ako predikatívne skutkové podstaty na účely trestného stíhania prania špinavých peňazí, a iba uvádzajú, že predikatívnymi skutkovými podstatami môžu byť všetky závažné trestné činy. Podľa odporúčaní FATF tieto zahŕňajú: časť v organizovanej zločineckej skupine a vydieranie, terorizmus vrátane financovania terorizmu, obchodovanie s ľuďmi a prevádzačstvo migrantov, sexuálne vykorisťovanie vrátane sexuálneho vykorisťovania detí, nezákonné obchodovanie s omamnými a psychotropnými látkami, nezákonné obchodovanie so zbraňami, nezákonné obchodovanie s kradnutým a iným tovarom, korupcia a úplatkárstvo, podvody, falšovanie peňazí, falšovanie a pirátstvo výrobkov, trestné činy proti životnému prostrediu, vražda, ťažké ublíženie na zdraví, únos, nezákonné obmedzovanie osobnej slobody a branie rukojemníkov, lúpež alebo krádež, pašovanie (vrátane colných a spotrebných daní a poplatkov), daňové trestné činy (súvisiace s priamymi a nepriamymi daňami), vydieranie, falšovanie, pirátstvo a obchodovanie s využitím dôverných informácií a manipulácia s trhom. Pri rozhodovaní o rozsahu trestných činov, ktoré budú zahrnuté ako predikatívne trestné činy v rámci každej z uvedených kategórií, sa každá krajina môže v súlade so svojím vnútroštátnym právom rozhodnúť, ako bude tieto trestné činy definovať a akú povahu budú mať jednotlivé prvky týchto trestných činov, ktoré z nich robia závažné trestné činy.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Kategória subjektov, na ktoré FATF rozšíril povinnosti AML/CFT nad rámec tradičného finančného sektora, keďže ich činnosť môže byť rovnako zneužitá na pranie špinavých peňazí alebo financovanie terorizmu ako služby finančných inštitúcií. FATF odporúčania (najmä odporúčania č. 22 a 23) zaraďujú do tejto kategórie nasledujúce subjekty:

a. **Kasína** – vrátane online kasín; vzhľadom na vysoký objem hotovostných transakcií a možnosť konverzie nelegálnych prostriedkov na výhry patria medzi najrizikové DNFBP.

b. **Realitné kancelárie** – pri sprostredkovaní nákupu a predaja nehnuteľností, ktoré sú klasickým nástrojom integrácie nelegálnych prostriedkov do legálnej ekonomiky.

c. **Obchodníci s drahými kovmi** – transakcie s zlatom, striebrom a inými drahými kovmi umožňujú efektívny prevod hodnôt mimo bankového systému.

d. **Obchodníci s drahými kameňmi** – diamanty a iné drahé kamene sú prenosné, hodnotné a ťažko sledovateľné, čo ich robí atraktívnym nástrojom prania špinavých peňazí.

e. **Právnici, notári, nezávislí právnici a účtovníci** – povinnosti AML/CFT sa vzťahujú na samostatne hospodáriacich odborníkov, partnerov a zamestnancov odborných firiem pri výkone špecifických činností, ako sú správa cudzích peňazí alebo majetku, zakladanie spoločností alebo trustov, nákup a predaj nehnuteľností alebo obchodných podielov a správa bankových, sporiacich alebo investičných účtov. Povinnosti sa nevzťahujú na interných profesionálov zamestnaných v iných podnikoch ani na odborníkov pracujúcich pre vládne agentúry. Osobitnou citlivou otázkou je vzťah AML/CFT povinností a právnej profesijnej mlčanlivosti (legal professional privilege) – väčšina jurisdikcií túto kolíziu rieši tak, že oznamovacia povinnosť sa nevzťahuje na informácie získané pri právnom zastupovaní klienta v súdnom konaní.

f. **Poskytovatelia dôveryhodnostných a firemných služieb (Trust and Company Service Providers – TCSP)** – ide o osoby alebo subjekty poskytujúce ako podnikateľskú činnosť tretím stranám niektorú z nasledujúcich služieb: zakladanie právnických osôb, výkon funkcie riaditeľa, tajomníka alebo spoločníka, poskytovanie sídla alebo korešpondenčnej adresy pre spoločnosti a iné právnické osoby, výkon funkcie správcu trustu alebo ekvivalentnej funkcie pri iných právnych zriadeniach a výkon funkcie nominálneho akcionára. TCSP sú osobitne rizikovými DNFBP, keďže ich služby sú priamo využívané na vytváranie nepriehľadných vlastníckych štruktúr zakrývajúcich skutočného vlastníka.

V kontexte AML/CFT je zaradenie DNFBP do regulačného rámca priamou reakciou na zistenie, že páchatelia systematicky využívali medzery medzi regulovaným finančným sektorom a neregulovanými profesijnými službami. Napriek tomu zostáva dohľad nad DNFBP vo väčšine jurisdikcií výrazne slabší ako dohľad nad finančnými inštitúciami, čo FATF vo svojich správach o vzájomnom hodnotení krajín opakovane identifikuje ako systémovú slabinu národných AML/CFT rámcov.

DESIGNATED PERSON OR ENTITY

Pojem určená osoba alebo subjekt sa vzťahuje na: jednotlivca, skupiny, podniky a subjekty označené výborom Bezpečnostnej rady zriadeným podľa rezolúcie 1267 (1999) (ďalej len „výbor 1267“) ako osoby spojené s al-Káidou alebo subjekty a iné skupiny a podniky spojené s al-Káidou; jednotlivci, skupiny, podniky a subjekty označené výborom Bezpečnostnej rady zriadeným podľa rezolúcie 1988 (2011) (ďalej len „výbor 1988“) ako osoby spojené s Talibanom, ktoré predstavujú hrozbu pre mier, stabilitu a bezpečnosť Afganistanu, alebo subjekty a iné skupiny a podniky spojené s Talibanom; akékoľvek fyzické alebo právnické osoby alebo subjekt, ktoré jurisdikcie alebo nadnárodné jurisdikcie určili podľa rezolúcie Bezpečnostnej rady 1373 (2001), akékoľvek fyzické alebo právnické osoby alebo subjekty určené na uplatňovanie cielených finančných sankcií podľa rezolúcie Bezpečnostnej rady 1718 (2006) a akýchkoľvek budúcich následných rezolúcií Bezpečnostnej rady v prílohách k príslušným rezolúciám alebo výboru Bezpečnostnej rady zriadeného podľa rezolúcie 1718 (2006) (sankčný výbor 1718) podľa rezolúcie Bezpečnostnej rady 1718 (2006) a akékoľvek fyzické alebo právnické osoby alebo subjekty určené na uplatňovanie cielených finančných sankcií podľa rezolúcie Bezpečnostnej rady 2231 (2015) a akýchkoľvek budúcich rezolúcií, ktoré ju nahradia.

DESIGNATION

Pojem sa vzťahuje na identifikáciu fyzickej alebo právnickej osoby alebo subjektu, na ktoré sa vzťahujú cielené finančné sankcie podľa rezolúcie Bezpečnostnej rady OSN č. 1267 (1999) a jej následných rezolúcií; rezolúcie Bezpečnostnej rady 1373 (2001) vrátane určenia, že sa na osobu alebo subjekt uplatnia príslušné sankcie, a verejného oznámenia tohto určenia; rezolúcia Bezpečnostnej rady 1718 (2006) a všetky budúce rezolúcie, ktoré ju nahradia; rezolúciu Bezpečnostnej rady 2231 (2015) a všetky budúce následné rezolúcie a všetky budúce rezolúcie Bezpečnostnej rady, ktorými sa ukladajú cielené finančné sankcie v súvislosti s financovaním šírenia zbraní hromadného ničenia. Pokiaľ ide o rezolúciu Bezpečnostnej rady 2231 (2015) a všetky budúce následné rezolúcie.

DILUTION OF SANCTIONED OWNERSHIP

Zložité vlastnícke štruktúry zahŕňajúce viacero subjektov v rôznych jurisdikciách môžu znížiť percentuálny podiel podniku, ktorý vlastní sankcionovaná strana, tak, že klesne pod prahové hodnoty, ktoré by bránili obchodovaniu. Toto oslabenie umožňuje sankcionovanej krajine alebo subjektu vyhnúť sa obmedzeniam, ktoré sankcie vytvárajú.

V kontexte AML/CFT a sankčného compliance predstavuje riedenie sankcionovaného vlastníctva jednu z najsofistikovanejších a najnebezpečnejších techník obchádzania sankcií, keďže priamo útočí na definičné kritériá sankčných predpisov. Väčšina sankčných režimov – vrátane OFAC v USA a sankčných nariadení EÚ – zakazuje transakcie so subjektmi, v ktorých sankcionovaná strana vlastní alebo kontroluje 50 % alebo viac (tzv. OFAC 50% Rule); riedením vlastníctva pod túto hranicu sa páchatelia snažia vytvoriť formálny súlad pri zachovaní faktickej kontroly sankcionovanej strany. Finančné inštitúcie sú preto povinné pri sankčnom screeningu neposudzovať len formálnu vlastnícku štruktúru, ale aktívne preskúmavať aj skutočnú kontrolu nad subjektom – vrátane nepriamych podielov, zmluvných práv, práv veta a iných mechanizmov kontroly – a pri komplexných štruktúrach s väzbami na sankcionované jurisdikcie aplikovať rozšírenú hĺbkovú previerku zameranú na odhalenie skrytých sankcionovaných vlastníkov bez ohľadu na výšku ich formálneho podielu.

DOLLAR CLEARING

Proces konverzie platieb klientov z cudzej meny na americké doláre.

V kontexte AML/CFT má dolárový klíring zásadný a často prehliadaný regulačný dosah – skutočnosť, že každá dolárová transakcia prechádza americkým bankovým systémom, automaticky zakladá jurisdikciu USA nad touto transakciou bez ohľadu na to, kde sa zmluvné strany nachádzajú. To znamená, že americké sankčné predpisy (OFAC) a požiadavky Bank Secrecy Act sa vzťahujú na všetky dolárové platby prechádzajúce cez americké korešpondenčné banky, vrátane transakcií medzi dvoma neamerickými subjektmi. Práve táto skutočnosť je základom extrateritoriálneho dosahu amerických sankcií a AML/CFT predpisov, ktorý výrazne ovplyvňuje správanie finančných inštitúcií po celom svete – banky mimo USA, ktoré chcú zachovať prístup k dolarovému klíringu, sú prakticky nútené dodržiavať americké sankčné a AML/CFT štandardy, keďže strata prístupu k dolarovému klíringu by pre väčšinu medzinárodne aktívnych inštitúcií znamenala faktické vylúčenie z globálneho finančného systému.

DOMESTIC TRANSFER

Elektronický prevod finančných prostriedkov, pri ktorom sa inštitúcie príkazcu a príjemcu nachádzajú v tej istej jurisdikcii. Tuzemský prevod sa preto vzťahuje na akýkoľvek reťazec bankových prevodov, ktorý sa uskutočňuje výlučne v rámci hraníc jednej jurisdikcie, aj keď skutočný systém použitý na odoslanie bankového prevodu sa môže nachádzať v inej jurisdikcii alebo online. Podľa FATF: Vzťahuje sa na akýkoľvek bankový prevod, pri ktorom sa finančná inštitúcia príkazcu a finančná inštitúcia príjemcu nachádzajú v tej istej krajine. Tento pojem sa teda vzťahuje na akýkoľvek reťazec bezhotovostného prevodu, ktorý sa uskutočňuje výlučne v rámci jednej krajiny, aj keď systém použitý na prevod platobnej správy sa môže nachádzať v inej krajine. Tento pojem sa vzťahuje aj na akýkoľvek reťazec bezhotovostného prevodu, ktorý sa celý uskutočňuje v rámci hraníc Európskeho hospodárskeho priestoru (EHP)[5] (ako sa tento pojem používa vo výkladovej poznámke k odporúčaniu FATF 16).

DUAL CONTROL

Zásada, podľa ktorej sú na splnenie úlohy vnútornej kontroly potrební najmenej dvaja zamestnanci. Účelom dvojitej kontroly je chrániť pred vnútornými podvodmi a zabrániť zlyhaniu vnútornej kontroly na jednom mieste. Označuje sa aj ako „tvorca - kontrolór“ alebo „štyri oči“.

V kontexte AML/CFT je dvojitá kontrola nevyhnutným prvkom integrity celého compliance procesu – uplatňuje sa najmä pri rozhodovaní o uzatvorení alebo zamietnutí alertov z transaction monitoringu, schvaľovaní rozhodnutí o nepodaní oznámenia o podozrivej aktivite (SAR/STR), vyhodnocovaní výsledkov hĺbkovej previerky klientov s vysokým rizikovým profilom, schvaľovaní onboardingu rizikových klientov vrátane PEP a klientov z vysoko rizikových jurisdikcií a pri realizácii transakcií nad stanovené limitné hodnoty. Absencia alebo obchádzanie princípu dvojitej kontroly v AML/CFT procesoch je pre regulátorov závažným varovným signálom naznačujúcim systémové zlyhanie vnútorných kontrol – práve koncentrácia rozhodovacej právomoci v rukách jednej osoby bez nezávislého overenia bola identifikovaná ako kľúčový faktor pri viacerých významných prípadoch prania špinavých peňazí, v ktorých compliance zamestnanci vedome alebo z nedbanlivosti zlyhali pri plnení svojich povinností.

DUAL-USE GOODS

Výrobky alebo technológie, ktoré možno použiť na obranné aj civilné účely. V diplomatických a politických platformách ide najčastejšie o tovar, ktorý môže slúžiť na viacero použití naraz. Príkladom je raketová technológia, ktorú možno použiť na vedecký výskum aj na obranné akcie alebo šifrovací softvér slúžiaci na ochranu súkromia aj na obrannú komunikáciu.

V kontexte AML/CFT a sankčného compliance predstavuje tovar s dvojakým použitím osobitnú výzvu práve pre svoju ambivalentnú povahu – legálna obchodná transakcia s civilným tovarom sa môže stať nástrojom obchádzania exportných kontrol, sankčných režimov a financovania proliferácie zbraní hromadného ničenia. Medzinárodné kontrolné režimy – Wassenaarovo dojednanie, Austrálska skupina, NSG a MTCR – definujú zoznamy kontrolovaného tovaru s dvojakým použitím, ktorých export podlieha licenčným povinnostiam; v EÚ je táto oblasť upravená nariadením o tovare s dvojakým použitím (2021/821). Pre finančné inštitúcie financujúce medzinárodný obchod vyplýva z tejto problematiky povinnosť identifikovať transakcie zahŕňajúce tovar s dvojakým použitím, overiť existenciu požadovaných exportných licencií, preskúmať deklarovaný účel použitia a konečného užívateľa (end-user) a posúdiť, či nedochádza k obchádzaniu exportných kontrol prostredníctvom falošného popisu tovaru alebo presmerovaním cez tretie krajiny – čo je zároveň typický vzorec Trade-Based Money Laundering a financovania proliferácie.

DUE DILIGENCE

Vyšetrovanie a preskúmanie spoločnosti alebo skupiny, ktoré sa vykonáva v procese prípravy obchodnej transakcie. Due diligence by sa mala vykonať pred uzavretím akejkoľvek finančnej transakcie alebo obchodného

[5] Subjekt môže požiadať FATF, aby bol označený za nadnárodnú jurisdikciu na účely a s obmedzením na posúdenie súladu s odporúčaním FATF 16.

vzťahu. V bežnom obchodnom chápaní ide o štandardnú prax pri fúziách, akvizíciách, investíciách alebo pri nadväzovaní obchodných partnerstiev.

V kontexte AML/CFT nadobúda pojem due diligence oveľa špecifickejší a záväznejší charakter – ide o právnu povinnosť zakotvenú v národnej AML/CFT legislatíve, smerniciach AMLD a odporúčaniach FATF, ktorá sa vzťahuje na všetky povinné osoby a zahŕňa tri úrovne intenzity prispôsobené rizikovému profilu klienta a obchodného vzťahu.

Štandardná hĺbková previerka (Customer Due Diligence – CDD) predstavuje základnú úroveň aplikovanú pri bežných klientoch a zahŕňa identifikáciu a overenie totožnosti klienta a skutočného vlastníka, pochopenie účelu a zamýšľanej povahy obchodného vzťahu a priebežné monitorovanie transakcií.

Zjednodušená hĺbková previerka (Simplified Due Diligence – SDD) je uplatniteľná pri klientoch, produktoch alebo transakciách s preukázateľne nízkym rizikom AML/CFT, kde postačujú menej prísne overovacie opatrenia.

Rozšírená hĺbková previerka (Enhanced Due Diligence – EDD) je povinná pri klientoch s vysokým rizikovým profilom – politicky exponovaných osobách (PEP), klientoch z vysoko rizikových jurisdikcií, korešpondenčných bankách a ďalších vysokorizikových kategóriách – a zahŕňa intenzívnejšie overovanie, hlbšie preskúmanie pôvodu majetku a prostriedkov a pravidelnejšie prehodnocovanie obchodného vzťahu.

Kľúčovým princípom AML/CFT due diligence je jej kontinuálna povaha – nejde o jednorazový proces pri otvorení účtu, ale o priebežnú povinnosť aktualizovať informácie o klientovi, sledovať zmeny v jeho rizikovom profile a reagovať na spúšťacie udalosti vyžadujúce opätovné overenie. Neschopnosť vykonať primeranú due diligence alebo udržiavať aktuálne informácie o klientovi patrí medzi najčastejšie sankcionované porušenia AML/CFT predpisov.

EASTERN AND SOUTHERN AFRICAN ANTI-MONEY LAUNDERING GROUP (ESAAMLG)

Skupina pre boj proti praniu špinavých peňazí východnej a južnej Afriky (ESAAMLG) je regionálny orgán, ktorý sa hlási ku globálnym štandardom boja proti praniu špinavých peňazí, financovaniu terorizmu a šíreniu zbraní. Jej 19 členskými krajinami sú Angola, Botswana, Eritrea, Eswatini, Etiópia, Keňa, Lesotho, Madagaskar, Malawi, Maurícius, Mozambik, Namíbia, Rwanda, Seychely, Južná Afrika, Tanzánia a Uganda, a Zimbabwe a zahŕňa množstvo regionálnych a medzinárodných pozorovateľov, ako napríklad AUSTRAC, sekretariát Commonwealthu, Východoafrické spoločenstvo, FATF, MMF, SADC, Spojené kráľovstvo, Spojené štáty americké, UNODC, Svetová banka a Svetová colná organizácia. Spojené kráľovstvo a Spojené štáty americké spolupracujú s organizáciou a podporujú ju od jej založenia v roku 1999.

ECONOMIC SANCTIONS

Uvalenie obchodných alebo finančných obmedzení a sankcií jednou alebo viacerými krajinami voči inej krajine, subjektu alebo jednotlivcovi s cieľom zmeniť ich správanie. Hospodárske sankcie môžu zahŕňať opatrenia, ako sú clá, obchodné obmedzenia a finančné obmedzenia.

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

Egmontská skupina ako celosvetová organizácia uľahčuje a podporuje výmenu informácií, poznatkov a spoluprácu medzi členskými finančnými spravodajskými jednotkami. Získajte prístup k základným dokumentom Egmont Group vrátane Charty a Zásad výmeny informácií medzi finančnými spravodajskými jednotkami. Skupina Egmont poskytuje finančným spravodajským jednotkám platformu na bezpečnú výmenu odborných znalostí a finančných spravodajských informácií na boj proti praniu špinavých peňazí, financovaniu terorizmu a súvisiacim predikatívnym trestným činom.

ELECTRONIC FUNDS TRANSFER (EFT)

Pohyb finančných prostriedkov medzi finančnými inštitúciami elektronicky. Dva najrozšírenejšie systémy elektronického prevodu finančných prostriedkov v USA sú FedWire a CHIPS (SWIFT sa často označuje ako tretí systém EFT, ale v skutočnosti ide o medzinárodný systém výmeny správ, ktorý prenáša pokyny na prevody medzi inštitúciami, a nie o samotný systém prevodov).

ELECTRONIC MONEY (E-MONEY)

Elektronická hotovosť predstavuje sériu peňažných jednotiek v určitom elektronickom formáte, napríklad elektronicky uložených online, na pevnom disku zariadenia alebo na mikročipe plastovej karty. V EÚ je vydávanie elektronických peňazí regulované smernicou o elektronických peniazoch (EMD2) a ich emitenti podliehajú licenčným požiadavkám.

V kontexte AML/CFT predstavujú elektronické peniaze dvojznačný nástroj – na jednej strane zvyšujú finančnú inklúziu a znižujú závislosť od ťažko sledovateľnej fyzickej hotovosti, na druhej strane anonymné alebo pseudonymné e-money produkty bez dostatočnej identifikácie používateľa môžu slúžiť ako náhrada hotovosti pri praní špinavých peňazí. Smernice AMLD preto stanovujú špecifické požiadavky na e-money produkty vrátane limitov pre anonymné používanie, povinnej identifikácie pri prekročení stanovených prahových hodnôt a zákazu anonymného dobíjania nad určitú sumu; 5AMLD tieto požiadavky výrazne sprísnila znížením limitov pre anonymné predplatené karty a rozšírením povinností na online e-money transakcie. Osobitnou výzvou je rastúce prelínanie tradičných e-money produktov s virtuálnymi aktívami a kryptomenami, kde hranica medzi regulovanými elektronickými peniazmi a neregulovanými virtuálnymi aktívami nie je vždy jednoznačná a vyžaduje si starostlivé právne posúdenie.

EMBARGO

Oficiálne vládne opatrenie na zákaz obchodu alebo obchodnej činnosti s určitou krajinou, ktoré sa niekedy týka konkrétneho obchodného produktu (napr. embargo na obilie alebo ropu).

EMBEZZLEMENT

Protiprávne konanie spočívajúce v odňatí alebo sprenevere finančných prostriedkov zverených zamestnávateľom alebo organizáciou pre vlastnú potrebu.

END-USER CERTIFICATE

Prepravný doklad, ktorým sa potvrdzuje, že kupujúci je konečným príjemcom materiálov a neplánuje ich previesť, reexportovať alebo inak odovzdať na inú tretiu stranu väčšinou bez predchádzajúceho súhlasu exportujúcej krajiny alebo výrobcu.

V kontexte AML/CFT a sankčného compliance predstavuje certifikát konečného užívateľa kľúčový, avšak inherentne zraniteľný kontrolný nástroj v systéme exportných kontrol – jeho hodnota závisí výlučne od pravdivosti deklarácií v ňom uvedených, pričom falšovanie alebo zneužívanie týchto certifikátov patrí medzi najrozšírenejšie techniky obchádzania exportných kontrol, sankčných režimov a financovania proliferácie zbraní hromadného ničenia. Typické vzorce zneužitia zahŕňajú uvedenie fiktívneho alebo bábkového konečného užívateľa v jurisdikcii bez exportných obmedzení s následným presmerovaním tovaru do sankcionovanej krajiny alebo k zakázanému konečnému užívateľovi, vystavenie certifikátu na legitímny civilný účel pri plánovanom obrannom využití tovaru s dvojakým použitím *(dual-use)* a využívanie reťazca sprostredkovateľov na rozptýlenie zodpovednosti a sťaženie sledovateľnosti. Pre finančné inštitúcie financujúce obchodné transakcie zahŕňajúce kontrolovaný tovar je preto nevyhnutné neposudzovať certifikát konečného užívateľa izolovane, ale v kontexte celkovej obchodnej transakcie – vrátane identity skutočného

konečného užívateľa, konzistentnosti deklarovaného účelu použitia s povahou tovaru, obchodných trás a zapojených jurisdikcií – a pri akýchkoľvek nezrovnalostiach aplikovať rozšírenú hĺbkovú previerku a zvážiť podanie oznámenia o podozrivej aktivite.

ENFORCEABLE MEANS

Pojem „vynútiteľné prostriedky" sa vzťahuje na nariadenia, usmernenia, pokyny alebo iné dokumenty či mechanizmy, ktoré stanovujú vynútiteľné požiadavky na boj proti praniu špinavých peňazí a financovaniu terorizmu v záväznom jazyku so sankciami za ich nedodržanie a ktoré vydal alebo schválil príslušný orgán. Sankcie za nedodržanie by mali byť účinné, primerané a odrádzajúce (pozri odporúčanie FATF 35) (ako sa tento pojem používa v poznámke o právnom základe požiadaviek na finančné inštitúcie a DNFBP).

ENHANCED DUE DILIGENCE (EDD)

V spojení s povinnou starostlivosťou o klienta EDD požaduje ďalšie opatrenia zamerané na identifikáciu a zmiernenie rizika, ktoré predstavujú rizikovejší klienti. Vyžaduje si vypracovanie dôkladnejších poznatkov o povahe klienta, jeho podnikaní a pochopenie transakcií na účte ako v prípade štandardného alebo menej rizikového klienta. Finančná inštitúcia by mala zabezpečiť aktuálnosť profilov účtov a monitorovanie by malo byť založené na riziku. Taktiež viď. definíciu Due Diligence.

EUROASIAN GROUP ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM (EAG)

Euroázijská skupina pre boj proti praniu špinavých peňazí a financovaniu terorizmu (EAG) je regionálny orgán na spôsob FATF, ktorý tvorí 9 krajín: Bielorusko, Čína, Kazachstan, Kirgizsko, India, Rusko, Tadžikistan, Turkménsko a Uzbekistan. Napriek tomu, že FATF vo februári 2023 pozastavil Rusku členstvo vo FATF, Rusko zostáva členom EAG. EAG je pridruženým členom FATF.

EUROPOL

Europol je agentúra EÚ na presadzovanie práva. Jeho hlavným cieľom je pomôcť dosiahnuť bezpečnejšiu Európu v prospech všetkých občanov EÚ. V oblasti boja proti praniu špinavých peňazí poskytuje Europol orgánom presadzovania práva členských štátov operačnú a analytickú podporu prostredníctvom styčných úradníkov Europolu (ELO) a svojich analytikov, ako aj najmodernejších databáz a komunikačných kanálov.

EVASION

Zámerné konanie smerujúce k vyhnutiu sa sankčným, regulačným alebo právnym povinnostiam s cieľom zapojiť sa do zakázanej činnosti bez odhalenia. V širšom právnom kontexte zahŕňa aj daňové úniky, obchádzanie exportných kontrol a iné formy zámerného porušovania zákonných povinností.

V kontexte AML/CFT predstavuje obchádzanie sankcií jedno z najzávažnejších porušení sankčného compliance s potenciálne devastujúcimi právnymi a reputačnými následkami pre finančné inštitúcie. Spektrum techník sankčného obchádzania je mimoriadne široké a neustále sa vyvíja – medzi najčastejšie patria stripping, teda odstraňovanie identifikačných informácií o sankcionovaných stranách z platobných správ pred ich odoslaním cez americký bankový systém, využívanie fronting companies a shell companies v nesankcionovaných jurisdikciách ako sprostredkovateľov zakrývajúcich skutočnú sankcionovanú protistranu, riedenie sankcionovaného vlastníctva pod prahové hodnoty (dilution of sanctioned ownership), falšovanie obchodnej dokumentácie vrátane certifikátov konečného užívateľa, využívanie virtuálnych aktív a mixérov na presun hodnôt mimo dosahu tradičného bankového systému a využívanie jurisdikcií ochotných ignorovať medzinárodné sankčné režimy ako prestupných uzlov pre zakázané transakcie. Pre finančné inštitúcie je obzvlášť dôležité pochopiť, že sankčné obchádzanie môže byť realizované aj bez ich vedomia – keď sú zneužité ako nevedomý sprostredkovateľ zakázanej transakcie; práve preto regulátori vyžadujú nielen reaktívne odhaľovanie porušení, ale aj proaktívne nastavenie kontrol schopných identifikovať indikátory potenciálneho obchádzania sankcií skôr, než k samotnému porušeniu dôjde.

EVENT-TRIGGERED MONITORING

Mechanismus riebežného monitorovania a prehodnocovania obchodných vzťahov aktivovaný konkrétnou udalosťou alebo zmenou v profile existujúceho klienta – na rozdiel od pravidelného periodického prehodnocovania, ktoré prebieha v stanovených časových intervaloch bez ohľadu na zmeny okolností.

V kontexte AML/CFT je monitorovanie spúšťané udalosťou kľúčovým prvkom dynamického prístupu k riadeniu rizík, ktorý reaguje na skutočnosť, že rizikový profil klienta sa môže kedykoľvek a nečakane zmeniť. Typickými spúšťacími udalosťami sú zmena jurisdikcie pôsobenia alebo sídla klienta, zmena vlastníckej štruktúry alebo skutočného vlastníka, zaradenie klienta alebo jeho spriaznenej osoby na sankčný zoznam, výrazná zmena v transakčnom správaní nezodpovedajúca pôvodnému profilu, mediálne správy o negatívnych zisteniach spojených s klientom (adverse media), zmena predmetu podnikania alebo vstup do vysoko rizikového sektora, politická expozícia klienta (získanie verejnej funkcie – vznik statusu PEP) a podanie trestného oznámenia alebo začatie vyšetrovania voči klientovi. Regulátori pri dohľadových inšpekciách osobitne posudzujú, či majú inštitúcie zavedené spoľahlivé systémy na zachytávanie spúšťacích udalostí v reálnom čase – nestačí spoliehať sa výlučne na periodické prehodnocovania, keďže riziko môže vzniknúť a materializovať sa v intervale medzi dvoma plánovanými kontrolami; absencia funkčného event-triggered monitoringu je preto považovaná za systémovú slabinu AML/CFT programu inštitúcie.

EXCLUSION LIST

Interný zoznam mien, subjektov alebo identifikátorov, ktoré boli compliance teamom preverené a preukázateľné overené ako nezhodujúce sa so sankcionovanými osobami alebo subjektmi na sankčných zoznamoch – napriek formálnej zhode mena alebo iných identifikátorov pri automatizovanom skríningu. Tieto záznamy sú následne vylúčené z opakovaného generovania alertov pri budúcich skríningových kontrolách.

V kontexte AML/CFT je zoznam vylúčených nevyhnutným praktickým nástrojom na riadenie vysokého objemu falošne pozitívnych výsledkov (false positives) generovaných automatizovanými sankčnými screeningovými systémami – bez jeho existencie by compliance tímy museli opakovane preverovať totožné záznamy, čo by neúmerne zaťažovalo kapacity a znižovalo celkovú účinnosť screeningového procesu. Napriek svojej praktickej nevyhnutnosti však zoznam vylúčených predstavuje potenciálne riziko, ktoré si vyžaduje prísne riadenie: každý záznam musí byť podložený zdokumentovaným a odôvodneným rozhodnutím o vylúčení, zoznamy musia byť pravidelne prehodnocované, keďže okolnosti odôvodňujúce vylúčenie sa môžu zmeniť, proces pridávania záznamov musí podliehať princípu dvojitej kontroly a schváleniu na primeranej úrovni riadenia, a systém musí zabezpečiť automatické odstránenie záznamu zo zoznamu vylúčených v prípade zmeny sankčného statusu danej osoby alebo subjektu; zneužitie alebo nedostatočné riadenie zoznamu vylúčených – napríklad pridávanie záznamov bez riadneho zdôvodnenia alebo zámerné vylučovanie skutočne sankcionovaných subjektov – môže viesť k závažným sankčným porušeniam a je predmetom osobitnej pozornosti regulátorov pri dohľadových inšpekciách.

EX PARTE

Pojem ex parte znamená konanie, rozhodnutie alebo príkaz vydaný súdom alebo príslušným orgánom bez predchádzajúceho oznámenia a účasti dotknutej strany.

V kontexte AML/CFT má konanie ex parte zásadný praktický význam pri niektorých z najcitlivejších nástrojov boja proti praniu špinavých peňazí a financovaniu terorizmu – príkazy na zmrazenie majetku, zaistenie dôkazov alebo odpočúvanie sú typicky vydávané práve ex parte, teda bez vedomia podozrivej osoby, keďže akékoľvek predchádzajúce oznámenie by mohlo viesť k úniku majetku, zničeniu dôkazov alebo úteku páchateľa. Rovnaký princíp stojí za zákazom tipping off v AML/CFT legislatíve – klient nesmie byť informovaný o podanom oznámení o podozrivej aktivite ani o prebiehajúcom vyšetrovaní, čo je v podstate aplikáciou princípu ex parte na úrovni finančnej inštitúcie. Pre finančné inštitúcie je dôležité pochopiť, že pri obdržaní ex parte príkazu od príslušných orgánov – napríklad príkazu na zmrazenie majetku alebo predloženie dokumentácie – sú povinné ho okamžite splniť a zároveň zachovať jeho dôvernosť voči dotknutému klientovi, pričom porušenie tejto povinnosti mlčanlivosti môže zmariť vyšetrovanie a zakladá trestnoprávnu zodpovednosť.

EXPORT ADMINISTRATION REGULATIONS (EAR)

Súbor predpisov, ktoré spravuje a presadzuje Úrad pre priemysel a bezpečnosť, oddelenie ministerstva obchodu USA. Vzťahujú sa konkrétne na fyzický tovar alebo komodity, ako sú technológie, softvér a iné položky podliehajúce kontrole vývozu.

EXPORT CONTROL JOINT UNIT (ECJU)

Agentúra so sídlom v Spojenom kráľovstve zodpovedná za správu licencií na kontrolovaný vývoz tovaru (vojenského a dvojakého použitia), na ktorý by sa inak mohlo vzťahovať embargo.

EXPRESS TRUST

Zverenecký fond vytvorený výslovne zriaďovateľom, zvyčajne vo forme dokumentu, ako je písomná zverenecká zmluva. Výslovný trust sa líši od trustov, ktoré nevyplývajú z konkrétneho zámeru alebo rozhodnutia zriaďovateľa vytvoriť trust (napr. konštruktívny trust zriadený súdom na riešenie nedeklarovaného majetku).

EXTERNAL EVASION

Situácia, keď klient alebo tretia strana obchádza sankčné povinnosti bez spolupráce alebo vedomia zamestnancov finančnej inštitúcie – inštitúcia je v takomto prípade zneužitá ako nevedomý nástroj sankčného porušenia.

V kontexte AML/CFT je rozlíšenie medzi externým a interným obchádzaním sankcií kľúčové z hľadiska právnej zodpovednosti inštitúcie – zatiaľ čo interné obchádzanie (za účasti zamestnancov) predstavuje závažné úmyselné porušenie s najvážnejšími právnymi dôsledkami, externé obchádzanie môže pri preukázaní dobrej viery a primeraných kontrol viesť k zmierneniu sankčného postihu. Regulátori a sankčné orgány – vrátane OFAC – však dôsledne posudzujú, či inštitúcia vynaložila primerané úsilie na predchádzanie externému obchádzaniu prostredníctvom robustného sankčného screeningu, transaction monitoringu, hĺbkovej previerky klientov a priebežného vzdelávania zamestnancov; samotná nevedomosť inštitúcie preto nie je automaticky obranou, ak boli jej kontrolné mechanizmy nedostatočné alebo ak existovali varovné signály, ktoré mali byť identifikované a vyhodnotené. Typickými indikátormi externého obchádzania sú neobvyklé platobné trasy prechádzajúce cez viacero jurisdikcií bez zjavného obchodného dôvodu, nekonzistentnosť medzi deklarovanou povahou transakcie a skutočnými peňažnými tokmi, využívanie fronting companies alebo sprostredkovateľov v nesankcionovaných krajinách a opakované transakcie s protistranami v blízkosti sankcionovaných jurisdikcií.

EXTRADICTION

Odovzdanie obvinenej alebo odsúdenej osoby jednou jurisdikciou druhej jurisdikcii na základe dohody, ktorá stanovuje podmienky takejto výmeny.

EXTRATERRITORIAL JURISDICTION (ETJ)

ETJ je právna možnosť vlády vykonávať právomoci za jej geopolitickými hranicami. Každý orgán si môže nárokovať ETJ nad akýmkoľvek vonkajším územím, ktoré si želá. Aby však bol tento nárok účinný na vonkajšom území (okrem uplatnenia sily), musí byť dohodnutý buď s právnym orgánom na vonkajšom území, alebo s právnym orgánom, ktorý pokrýva obe územia. Ak sa ETJ nekvalifikuje, zvyčajne sa vzťahuje na takúto dohodnutú jurisdikciu, alebo sa nazýva nejako ako „nárokovaná ETJ“. Toto slovné spojenie sa môže vzťahovať aj na právne predpisy krajiny, ktoré presahujú jej hranice v tom zmysle, že môžu oprávňovať súdy tejto krajiny, aby uplatňovali svoju právomoc voči stranám, ktoré pred nimi vystupujú, v súvislosti s úkonmi, ktorých sa údajne dopustili mimo tejto krajiny. To nezávisí od spolupráce iných krajín, keďže dotknuté osoby sa nachádzajú na území príslušnej krajiny (alebo aspoň v prípade, že ide o osobu, ktorá je súdená v neprítomnosti, vec prejednáva súd tejto krajiny). Mnohé krajiny majú napríklad zákony, na základe ktorých majú ich trestné súdy právomoc súdiť trestné stíhanie za pirátstvo, sexuálne trestné činy proti deťom, počítačové trestné činy a/alebo terorizmus spáchané mimo hraníc ich štátu. Niekedy sa takéto zákony vzťahujú len na štátnych príslušníkov danej krajiny a niekedy sa môžu vzťahovať na kohokoľvek.

EXTRATERRITORIAL REACH

Rozšírenie politiky a právnych predpisov jednej krajiny na občanov a inštitúcie inej krajiny. Ide o uplatňovanie právnych predpisov a regulačných požiadaviek jednej krajiny na subjekty, transakcie alebo konanie, ktoré sa odohrávajú mimo jej územia – vrátane cudzích štátnych príslušníkov a zahraničných inštitúcií, ktoré nemajú priame sídlo ani pobočku v danej krajine.

V kontexte AML/CFT má extrateritoriálny dosah najvýraznejší praktický dopad v prípade USA, ktorých sankčné a AML/CFT predpisy de facto stanovujú globálne štandardy pre všetky inštitúcie zapojené do dolárového klíringu alebo majúce akýkoľvek kontakt s americkým finančným systémom. Právnym základom tohto dosahu je kombinácia niekoľkých mechanizmov – dolárový klíring zakladá jurisdikciu USA nad každou dolárovou transakciou bez ohľadu na miesto jej pôvodu, korešpondenčné bankové vzťahy s americkými bankami zaväzujú zahraničné inštitúcie dodržiavať americké štandardy, a sankčné predpisy OFAC sa vzťahujú na akúkoľvek transakciu prechádzajúcu americkým finančným systémom alebo zahŕňajúcu americké osoby. Sekundárne sankcie USA idú ešte ďalej – postihujú aj subjekty tretích krajín obchodujúce so sankcionovanými krajinami či osobami, aj keď nemajú žiadne priame prepojenie na USA. Extrateritoriálny dosah americkej legislatívy bol základom niekoľkých historicky najvyšších pokút udelených zahraničným bankám za porušenie sankčných predpisov – vrátane prípadov BNP Paribas (8,9 mld. USD), HSBC alebo Standard Chartered – a zásadne ovplyvňuje správanie finančných inštitúcií po celom svete, ktoré sú prakticky nútené dodržiavať americké AML/CFT a sankčné štandardy ako podmienku prístupu ku globálnemu finančnému systému.

FACILITATION (UĽAHČENIE/NAPOMÁHANIE)

Činnosti, ktoré vykonáva jedna osoba na pomoc alebo podporu inej osoby pri vykonávaní činnosti. V kontexte sankcií uľahčenie znamená, že jedna osoba (osoba A), ktorá sa nesmie zapojiť do činnosti, priamo alebo nepriamo pomáha inej osobe (osoba B) alebo ju podporuje, aby sa zapojila do tejto činnosti. Táto činnosť nemusí byť nevyhnutne zakázaná pre osobu B, ale len pre osobu A.

V kontexte AML/CFT a sankčného compliance predstavuje uľahčenie jeden z najširších a najdôležitejších konceptov zodpovednosti – sankčné predpisy väčšiny jurisdikcií výslovne zakazujú nielen priame porušenie sankcií, ale aj akékoľvek napomáhanie, podporu alebo umožnenie obchádzania sankcií inými osobami. Pre finančné inštitúcie to znamená, že aj transakcia, ktorá sama osebe nie je priamym porušením sankcií, môže

zakladať sankčnú zodpovednosť, ak inštitúcia vedela alebo mala vedieť, že uľahčuje sankcionovanej strane prístup k finančnému systému prostredníctvom tretej osoby. Typickými príkladmi uľahčenia sú spracovanie platby pre nesankcionovanú spoločnosť, ktorá koná v mene sankcionovaného subjektu, poskytovanie finančných služieb sprostredkovateľovi, ktorého skutočným klientom je sankcionovaná osoba, a vykonávanie transakcií štruktúrovaných tak, aby umožnili sankcionovanej strane nepriamy prístup k finančnému systému. Zákaz uľahčenia je tiež kľúčovým prvkom trestnoprávnej zodpovednosti za pranie špinavých peňazí – pomocník alebo spolupáchateľ, ktorý vedome uľahčuje pranie špinavých peňazí bez priamej účasti na predikátnom trestnom čine, môže byť trestne zodpovedný rovnako ako priamy páchateľ, čo je explicitne zakotvené v 6AMLD a v trestných zákonníkoch väčšiny jurisdikcií.

FALSE DECLARATION

Týka sa nesprávneho uvedenia hodnoty prepravovanej meny alebo BNI alebo nesprávneho uvedenia iných relevantných údajov, ktoré sa vyžadujú na predloženie v colnom vyhlásení alebo ktoré si orgány inak vyžiadajú. Patrí sem aj nepodanie požadovaného vyhlásenia (ako sa tento pojem používa vo výkladovej poznámke k odporúčaniu FATF 32).

FALSE DISCLOSURE

Vzťahuje sa na skreslenie hodnoty prepravovanej meny alebo BNI alebo na skreslenie iných relevantných údajov, ktoré sa požadujú na základe žiadosti o zverejnenie alebo ktoré si inak vyžiadajú orgány. Patrí sem aj nezverejnenie požadovaných údajov (ako sa tento pojem používa vo výkladovej poznámke k odporúčaniu FATF 32).

FALSE NEGATIVE

Situácia, keď screeningový alebo monitorovací systém neidentifikuje skutočnú zhodu alebo skutočné podozrivé správanie, ktoré malo byť zachytené. Môže nastať v dvoch formách: ako nesprávne zamietnutie skutočnej zhody so sankčným zoznamom počas preverovanie alertu, alebo ako systémové zlyhanie kalibrácie, keď sú prahové hodnoty nastavené príliš vysoko a skutočné hodnoty nie sú vôbec generované ako alerty.

V kontexte AML/CFT predstavuje falošne negatívny výsledok oveľa závažnejšie riziko ako jeho opak – falošne pozitívny výsledok (false positive) – keďže znamená, že sankcionovaná osoba, podozrivá transakcia alebo pranie špinavých peňazí prešli bez povšimnutia cez kontrolné mechanizmy inštitúcie. Zatiaľ čo vysoký počet falošne pozitívnych výsledkov zaťažuje kapacity compliance tímu, vysoký počet falošne negatívnych výsledkov priamo ohrozuje integritu celého AML/CFT programu a môže viesť k závažným regulačným porušeniam. Regulátori pri dohľadových inšpekciách osobitne skúmajú mieru falošne negatívnych výsledkov prostredníctvom back-testingu – testovania, či by historické transakcie alebo klienti so známymi sankčnými alebo AML/CFT problémami boli zachytení existujúcimi kontrolnými mechanizmami; vysoká miera falošne negatívnych výsledkov je priamym dôkazom nedostatočnej kalibrácie systémov a nedostatočnej účinnosti AML/CFT programu. Finančné inštitúcie sú preto povinné pravidelne testovať a prehodnocovať nastavenie prahových hodnôt svojich screeningových a monitorovacích systémov s cieľom nájsť optimálnu rovnováhu medzi minimalizáciou falošne negatívnych výsledkov a udržateľným objemom falošne pozitívnych výsledkov.

FALSE POSITIVE

Zhoda identifikovaná počas procesu preverovania ako možné varovanie *(alert),* ale po preskúmaní sa zistí, že sa nezhoduje s cieľom uvedeným na sankčnom zozname.

V kontexte AML/CFT je miera falošne pozitívnych výsledkov jednou z najvýznamnejších operačných výziev compliance funkcií finančných inštitúcií – v praxi tvoria falošne pozitívne výsledky drvivú väčšinu všetkých generovaných alertov, pričom v niektorých inštitúciách presahuje ich podiel 95 % všetkých záchytov. Vysoký objem falošne pozitívnych výsledkov má priame negatívne dôsledky: zaťažuje kapacity compliance tímu rutinným preverovaním nerelevantných alertov na úkor hlbšej analýzy skutočne rizikových prípadov, zvyšuje prevádzkové náklady, môže viesť k oneskoreným alebo zablokovaným legitímnym transakciám poškodzujúcim klientov a pri chronickom preťažení analytikov zvyšuje riziko, že skutočná zhoda bude prehliadnutá. Regulátori však zároveň dôsledne sledujú, aby snaha o zníženie miery falošne pozitívnych výsledkov neviedla k neprimeranému zvyšovaniu prahových hodnôt a následnému nárastu falošne negatívnych výsledkov – optimálna kalibrácia systému musí nájsť rovnováhu medzi operačnou efektívnosťou a schopnosťou zachytiť skutočné porušenia. Moderné prístupy k redukcii falošne pozitívnych výsledkov zahŕňajú využívanie umelej inteligencie a strojového učenia na inteligentnejší scoring alertov, rozšíreného kontextuálneho skórovania zohľadňujúceho viacero identifikačných atribútov súčasne a pravidelné prehodnocovanie a ladenie parametrov screeningových modelov.

FINAL RULE PART 504

Predpisy, ktoré 30. júna 2016 vydalo Ministerstvo finančných služieb štátu New York (DFS) s cieľom zdôrazniť potrebu spoľahlivých programov monitorovania a filtrovania transakcií (TMP). Predpis nadobudol účinnosť 1. januára 2017 a vyžaduje, aby regulované inštitúcie udržiavali TMP primerane navrhnuté na monitorovanie transakcií po ich vykonaní z hľadiska súladu so zákonom o bankovom tajomstve a zákonmi a nariadeniami o boji proti praniu špinavých peňazí a pred ich vykonaním z hľadiska súladu s Úradom ministerstva financií USA pre kontrolu zahraničných aktív (OFAC). Nariadenie zahŕňa požiadavky na oznamovanie podozrivých činností a prevenciu nezákonných transakcií s cieľmi ekonomických sankcií spravovaných OFAC.

FINANCIAL GROUP

Finančná skupina znamená skupinu subjektov, ktorá pozostáva z materskej spoločnosti alebo z akéhokoľvek iného typu právnickej osoby, ktorá vykonáva kontrolné a koordinačné funkcie nad zvyškom skupiny na účely uplatňovania dohľadu nad skupinou podľa základných zásad, spolu s pobočkami a/alebo dcérskymi spoločnosťami, ktoré podliehajú politikám a postupom AML/CFT na úrovni skupiny. Materská spoločnosť zodpovedá za dohľad nad implementáciou skupinových štandardov v súlade so základnými princípmi prudenciálneho dohľadu.

V kontexte AML/CFT má koncept finančnej skupiny zásadný regulačný význam – odporúčania FATF (najmä odporúčanie č. 18) a smernice AMLD vyžadujú, aby finančné skupiny implementovali AML/CFT politiky a postupy na úrovni celej skupiny, vrátane politík zdieľania informácií v rámci skupiny na účely AML/CFT, jednotných štandardov KYC/CDD a skupinových programov hodnotenia rizík. Kľúčovou výzvou je skutočnosť, že jednotlivé subjekty skupiny pôsobia v rôznych jurisdikciách s odlišnými regulačnými požiadavkami – tam, kde miestne požiadavky presahujú skupinové štandardy, musia byť uplatnené prísnejšie miestne požiadavky, a naopak, tam, kde miestne predpisy neumožňujú implementáciu skupinových štandardov, napríklad z dôvodu obmedzení zdieľania informácií alebo bankového tajomstva, je materská spoločnosť povinná o tejto skutočnosti informovať príslušné orgány domovskej jurisdikcie. Regulátori pri dohľade nad finančnými skupinami osobitne posudzujú konzistentnosť AML/CFT štandardov naprieč celou skupinou, kvalitu skupinového dohľadu nad dcérskymi spoločnosťami v jurisdikciách s vyšším rizikom a schopnosť materskej spoločnosti identifikovať a riadiť AML/CFT riziká na konsolidovanom základe.

FINANCIAL INSTITUTION

Finančné inštitúcie sú všetky fyzické alebo právnické osoby, ktoré vykonávajú jednu alebo viacero z nasledujúcich činností alebo operácií pre

klienta alebo v jeho mene: prijímanie vkladov a iných návratných finančných prostriedkov od verejnosti[6], poskytovanie úverov[7], finančný lízing[8], služby prevodu peňazí alebo hodnôt[9], vydávanie a správa platobných prostriedkov (napr. kreditných a debetných kariet, šekov, cestovných šekov, peňažných poukážok a bankových zmeniek, elektronických peňazí), finančné záruky a záväzky, obchodovanie s finančnými prostriedkami: (a) nástroje peňažného trhu (šeky, zmenky, vkladové certifikáty, deriváty atď.), (b) devízových kurzov, (c) devízové, úrokové a indexové nástroje, (d) prevoditeľné cenné papiere, a (e) obchodovanie s komoditnými futures, ďalej účasť na emisiách cenných papierov a poskytovanie finančných služieb súvisiacich s týmito emisiami, individuálna a kolektívna správa portfólia, úschova a správa peňažných prostriedkov alebo likvidných cenných papierov na účet iných osôb, iné investovanie, správa alebo hospodárenie s finančnými prostriedkami alebo peniazmi v mene iných osôb, upisovanie a umiestňovanie životného poistenia a iných poistení súvisiacich s investovaním[10], a zmeny peňazí a meny.

FINANCIAL ACTION TASK FORCE (FATF)

FATF bola založená v roku 1989 skupinou siedmich priemyselných štátov s cieľom podporiť zavedenie vnútroštátnych a globálnych opatrení na boj proti praniu špinavých peňazí. Je to medzinárodný politický orgán, ktorý stanovuje normy proti praniu špinavých peňazí a opatrenia proti financovaniu terorizmu na celom svete. Jej odporúčania nemajú silu zákona. Jej členmi je 38 členských jurisdikcií a dve medzinárodné organizácie (Európska komisia a GCC). V roku 2012 FATF podstatne revidovala svojich 40 + 9 odporúčaní a zredukovala ich na 40. Vo februári 2023 FATF pozastavil členstvo Rusku (z dôvodov invázie na Ukrajinu). FATF každoročne vypracúva typologické správy, v ktorých prezentuje aktuálne trendy a metódy prania špinavých peňazí a financovania terorizmu.

FATF RECOMMENDATIONS

Úplný súbor opatrení proti praniu špinavých peňazí, ktoré zahŕňajú systém trestného súdnictva a presadzovania práva, finančný systém a jeho reguláciu a medzinárodnú spoluprácu, ktoré vydáva FATF.

Financial Action Task Force on Money Laundering in Latin America (GAFILAT)

Cieľom Finančnej akčnej skupiny Latinskej Ameriky (GAFILAT) (predtým známej ako Finančná akčná skupina Južnej Ameriky (GAFISUD)) je pracovať na vypracovaní a implementácii komplexnej globálnej stratégie boja proti praniu špinavých peňazí a financovaniu terorizmu, ako je stanovené v odporúčaniach FATF. Toto úsilie zahŕňa podporu vytvorenia trestného činu prania špinavých peňazí v súvislosti so závažnými trestnými činmi, rozvoj právnych systémov na účinné vyšetrovanie a stíhanie týchto trestných činov, vytvorenie systémov na oznamovanie podozrivých transakcií, podporu vzájomnej právnej pomoci. GAFILAT tiež podporuje odbornú prípravu osôb zapojených do boja proti praniu špinavých peňazí. GAFILAT umožňuje zohľadniť regionálne faktory pri vykonávaní opatrení proti praniu špinavých peňazí.

Počiatky GAFILAT siahajú k prebiehajúcemu úsiliu o integráciu úsilia v oblasti boja proti praniu špinavých peňazí v Južnej Amerike a podnietilo ho vytvorenie iných regionálnych skupín pre boj proti praniu špinavých peňazí, ktoré boli založené podľa vzoru FATF. Vznikla ako GAFISUD 8. decembra 2000 v Cartagene v Kolumbii na základe memoranda o porozumení zástupcov vlád deviatich juhoamerických krajín. Organizácia amerických štátov (OAS) je tiež členom s poradnou funkciou prostredníctvom Medziamerickej komisie proti zneužívaniu drog (CICAD). Po udalostiach z 11. septembra 2001 GAFISUD rozšíril svoju pôsobnosť o boj proti financovaniu terorizmu. Na plenárnom zasadnutí GAFISUD, ktoré sa konalo 7. - 11. júla 2014, bola schválená zmena názvu z GAFISUD na GAFILAT, aby sa zohľadnilo rozšírenie jeho členstva na všetky latinskoamerické krajiny. GAFILAT sa zaviazal vykonávať vzájomné hodnotenia a koordinovať školenia a vzdelávacie aktivity v oblasti boja proti praniu špinavých peňazí v regióne. Jej pracovný mandát je stanovený v memorande o porozumení, ktoré obsahuje konkrétne kompetencie skupiny. Skupinu GAFILAT podporuje sekretariát, ktorý slúži ako kontaktné miesto pre jej činnosti. GAFILAT sa stal pridruženým členom FATF v roku 2006.

FINANCIAL ACTION TASK FORCE-STYLE REGIONAL BODY (FSRB)

9 regionálnych orgánov typu FATF (FSRB) je autonómnych regionálnych organizácií, ktoré pomáhajú Finančnej akčnej skupine (FATF) implementovať jej globálnu politiku boja proti praniu špinavých peňazí a financovaniu terorizmu, ktorá sa zakladá na 40 odporúčaniach, vo viac ako 200 pridružených krajinách. FATF je najvýznamnejším svetovým regulačným orgánom v oblasti boja proti praniu špinavých peňazí (AML) a financovania terorizmu (CFT). Hoci má 39 oficiálnych členov a jurisdikcií, závisí od podpory deviatich regionálnych orgánov typu FATF (FSRB), aby sa zabezpečilo, že jeho politiky sa rozšíria do všetkých kútov sveta.

FINANCIAL INTELLIGENCE UNIT (FIU)

Centrálna národná agentúra zodpovedná za prijímanie, analýzu a odovzdávanie informácií o podozrivých transakciách príslušným orgánom. FIU predstavuje kľúčový článok medzi povinným sektorom a orgánmi presadzovania práva.

V kontexte AML/CFT zohráva FIU nezastupiteľnú úlohu v národnom aj medzinárodnom systéme boja proti praniu špinavých peňazí a financovaniu terorizmu. Odporúčanie FATF č. 29 explicitne vyžaduje, aby každá krajina zriadila funkčnú FIU ako autonómny orgán s operačnou nezávislosťou. FIU môže byť organizovaná v štyroch modeloch – súdnom, policajnom, administratívnom alebo hybridnom – pričom najrozšírenejším v EÚ je administratívny model, kde FIU nie je priamo súčasťou polície ani prokuratúry, čo jej umožňuje prijímať informácie od povinného sektora bez automatického spúšťania trestného konania. Okrem prijímania a analýzy SAR/STR plní FIU ďalšie kľúčové funkcie – strategickú analýzu typológií a trendov prania špinavých peňazí, operatívnu analýzu konkrétnych prípadov na základe krížovej kontroly s dostupnými databázami, spätnú väzbu smerom k povinným osobám o kvalite a využiteľnosti podaných oznámení a medzinárodnú výmenu finančných spravodajských informácií prostredníctvom siete Egmont Group, ktorá združuje FIU z viac ako 160 krajín. Efektívnosť FIU je jedným z kľúčových ukazovateľov hodnotených pri vzájomných hodnoteniach FATF – krajiny s nedostatočne vybavenými, personálne poddimenzovanými alebo politicky závislými FIU dostávajú nízke hodnotenia účinnosti bez ohľadu na formálnu kvalitu ich AML/CFT legislatívy.

FINANCIAL SECTOR ASSESSMENT PROGRAMME (FSAP)

Program hodnotenia finančného sektora (FSAP), ktorý bol zavedený v roku 1999, predstavuje komplexné a hĺbkové hodnotenie finančného sektora krajiny. FSAP vo vyspelých ekonomikách vykonáva MMF so zameraním

[6] Táto položka zachytáva aj súkromné bankovníctvo.

[7] Patria sem okrem iného: spotrebiteľské úvery; hypotekárne úvery; faktoring s regresom alebo bez regresu a financovanie obchodných transakcií (vrátane forfeitingu).

[8] Nepatria sem dohody o finančnom lízingu v súvislosti so spotrebiteľskými produktmi.

[9] Nevzťahuje sa na žiadnu fyzickú alebo právnickú osobu, ktorá poskytuje finančným inštitúciám výlučne systémy správ alebo iné podporné systémy na prenos finančných prostriedkov. Pozri výkladovú poznámku k odporúčaniu FATF 16.

[10] To sa vzťahuje na poisťovne aj na sprostredkovateľov poistenia (agentov a maklérov).

na hodnotenie odolnosti finančného sektora, kvality regulačného rámca a rámca dohľadu a schopnosti riadiť a riešiť finančné krízy. V rozvojových a rozvíjajúcich sa trhových ekonomikách sa FSAP vykonávajú spoločne so Svetovou bankou. Súčasťou týchto FSAP je aj hodnotenie finančného rozvoja, za ktoré zodpovedá Svetová banka. Na základe zistení FSAP sa vypracúvajú odporúčania mikro- a makroprudenciálnej povahy a odporúčania týkajúce sa rozvojových potrieb v rozvojových a rozvíjajúcich sa trhových ekonomikách, ktoré sú prispôsobené podmienkam konkrétnej krajiny. Tieto odporúčania sú obsiahnuté v Aide Memoire, čo je dôverný a komplexný dokument, ktorý sa ponecháva vnútroštátnym orgánom na konci poslednej misie FSAP. FSAP sa končia prípravou hodnotenia stability finančného systému (Financial System Stability Assessment - FSSA), ktoré sa prerokúva vo Výkonnej rade MMF spolu so správou krajiny podľa článku IV. Zverejnenie FSSA sa predpokladá, ale je dobrovoľné. Okrem hlavného dokumentu (uvedeného nižšie, ak bol zverejnený) môžu jednotlivé krajiny v rámci FSAP predložiť ďalšie podporné dokumenty. FSAP je kľúčovým nástrojom dohľadu fondu a poskytuje dôležité vstupy pre bilaterálny dohľad v kontexte konzultácií podľa článku IV. Hodnotenie finančnej stability v rámci FSAP je povinnou súčasťou dohľadu podľa článku IV pre členov so systémovo dôležitým finančným sektorom (SIFS) a v súčasnosti sa očakáva, že sa uskutoční každých päť alebo desať rokov v závislosti od ich relatívneho systémového významu pri prenose šokov cez hranice; pre všetky ostatné jurisdikcie je účasť v programe dobrovoľná.

FINANCIAL STABILITY BOARD (FSB)

Medzinárodný orgán, ktorý monitoruje a vydáva odporúčania týkajúce sa globálneho finančného systému. FSB koordinuje národné finančné orgány a medzinárodné štandardizačné subjekty pri vytváraní silných regulačných, dozorných a iných politík finančného sektora. Spolupracuje s FATF pri riešení rizík finančnej stability spojených s praním špinavých peňazí a financovaním terorizmu.

FINTECH (FINANCIAL TECHNOLOGY)

Technologické inovácie v oblasti finančných služieb, ktoré zahŕňajú digitálne platby, peer-to-peer pôžičky, robo-poradcov, blockchain a ďalšie. Z pohľadu AML/CFT predstavuje FinTech nové výzvy (anonymita, rýchlosť transakcií, cezhraničný charakter) aj príležitosti (pokročilá analytika, automatizovaný screening). Regulátori vyžadujú od FinTech spoločností plnenie rovnakých AML/CFT povinností ako od tradičných finančných inštitúcií.

FIRST LINE OF DEFENSE

V rámci riadiacej štruktúry programu dodržiavania sankcií patrí do prvej línie obrany (označovanej aj ako „prvá línia“) manažéri vzťahov a iní zamestnanci, ktorí sú najbližšie ku klientom a protistranám vo fáze nadväzovania vzťahov a uzatvárania zmlúv. Prvá línia obrany je zodpovedná za zabezpečenie získania adekvátnych informácií, aby bolo možné vykonať účinnú kontrolu zákazníkov a ich vlastníkov a správcov. Vo všeobecnosti platí, že obrana prvej línie vlastní a riadi zber informácií o SDD.

FOLLOW-UP REPORTS

Správy členských štátov EAG o zlepšeniach vnútroštátneho režimu AML/CFT, ktoré boli vykonané na základe odporúčaní vypracovaných na základe výsledkov vzájomného hodnotenia.

FOREIGN COUNTERPARTS

Zahraničnými partnermi sa rozumejú zahraničné príslušné orgány, ktoré vykonávajú podobné povinnosti a funkcie vo vzťahu k spolupráci, o ktorú sa žiada, a to aj v prípade, že tieto zahraničné príslušné orgány majú odlišnú povahu alebo postavenie (napr. v závislosti od krajiny môže dohľad nad AML/CFT v určitých finančných sektoroch vykonávať orgán dohľadu, ktorý má aj povinnosti prudenciálneho dohľadu, alebo útvar dohľadu FIU).

FOREIGN SANCTIONS EVADER (FSE)

Zahraničná fyzická alebo právnická osoba, o ktorej sa zistilo, že porušila, pokúsila sa porušiť, konšpirovala s cieľom porušiť alebo spôsobila porušenie sankcií USA. OFAC zverejňuje zoznam FSE a transakcie osôb z USA alebo v rámci USA, ktoré sa týkajú FSE, sú zakázané.

FORFEITURE

Nedobrovoľná strata majetku alebo aktív v dôsledku súdneho konania. Vo všeobecnosti ide o prípad, keď vlastník majetku nedodržal zákon alebo keď je majetok spojený s nejakou trestnou činnosťou.

FREE TRADE ZONE (FTZ)

Zóny FTZ (zóny voľného obchodu), známe aj ako osobitné hospodárske zóny, sú vymedzené geografické oblasti v rámci krajiny so správou zóny, ktorá poskytuje infraštruktúru a služby nájomným spoločnostiam. Vo FTZ platia odlišné pravidlá podnikania, ktoré sú podporované súborom politických nástrojov, ktoré nie sú všeobecne platné pre zvyšok krajiny. Zóny voľného obchodu predstavujú kľúčovú rizikovú oblasť špecifickú pre činnosti súvisiace s obchodom, pretože sa v nich bežne uplatňujú neprimerané sankčné záruky, miestnymi orgánmi sa vykonáva len minimálny dohľad, postupy kontroly tovaru a právnických osôb sú slabé vrátane vhodných systémov vedenia záznamov a informačných technológií, a chýba spolupráca medzi zónami voľného obchodu a miestnymi colnými orgánmi.

FREEZE

Zabrániť alebo obmedziť výmenu, výber, likvidáciu alebo používanie aktív alebo bankových účtov. Na rozdiel od konfiškácie zmrazený majetok, vybavenie, finančné prostriedky alebo iné aktíva zostávajú majetkom fyzickej alebo právnickej osoby (osôb), ktorá (ktoré) o ne mala (mali) záujem v čase zmrazenia, a môžu ich naďalej spravovať tretie strany. Súdy môžu rozhodnúť o zmrazení ako o prostriedku ochrany pred útekom. Podľa FATF odporúčaní: V kontexte konfiškácie a predbežných opatrení (napr. odporúčania FATF 4, 32 a 38) pojem „zmrazenie“ znamená zákaz prevodu, premeny, disponovania alebo pohybu akéhokoľvek majetku, zariadenia alebo iných nástrojov na základe a počas trvania platnosti konania iniciovaného príslušným orgánom alebo súdom v rámci mechanizmu zmrazenia, alebo kým príslušný orgán nerozhodne o prepadnutí alebo konfiškácii. Na účely odporúčaní 6 a 7 o vykonávaní cielených finančných sankcií sa pod pojmom zmrazenie rozumie zákaz prevodu, konverzie, disponovania alebo pohybu akýchkoľvek finančných prostriedkov alebo iných aktív, ktoré sú vo vlastníctve alebo pod kontrolou určených osôb alebo subjektov, na základe a počas platnosti opatrenia iniciovaného Bezpečnostnou radou OSN alebo v súlade s platnými rezolúciami Bezpečnostnej rady príslušným orgánom alebo súdom. Vo všetkých prípadoch zmrazený majetok, vybavenie, nástroje, finančné prostriedky alebo iné aktíva zostávajú majetkom fyzickej alebo právnickej osoby (osôb), ktorá (ktoré) na nich mala (mali) záujem v čase zmrazenia, a môžu byť naďalej spravované tretími stranami alebo prostredníctvom iných dohôd, ktoré takáto fyzická alebo právnická osoba (osoby) uzavrela (uzavreli) pred začatím konania na základe mechanizmu zmrazenia alebo v súlade s inými vnútroštátnymi ustanoveniami. V rámci vykonávania zmrazenia sa krajiny môžu rozhodnúť prevziať kontrolu nad majetkom, vybavením, nástrojmi alebo finančnými prostriedkami alebo inými aktívami ako prostriedok ochrany pred únikom.

FRONT COMPANY

Akýkoľvek podnik zriadený a kontrolovaný inou organizáciou. Hoci to nemusí byť nevyhnutne nezákonné, páchatelia využívajú krycie spoločnosti na pranie špinavých peňazí tým, že im dávajú zdanie legitímneho pôvodu. Krycie spoločnosti môžu dotovať výrobky a služby na úrovni výrazne nižšej, ako sú trhové sadzby, alebo dokonca pod úrovňou výrobných nákladov.

V kontexte AML/CFT plní krycí podnik niekoľko kľúčových funkcií v procese prania špinavých peňazí – poskytuje zdanie legitímneho obchodného pôvodu pre nelegálne prostriedky, umožňuje miešanie nelegálnych príjmov s legitímnymi tržbami (asset mingling), zakrýva totožnosť skutočného vlastníka a vytvára vrstvu falošnej legitimity medzi nelegálnym zdrojom prostriedkov a ich konečným užívateľom. Typickými znakmi krycieho podniku sú absencia reálnej obchodnej činnosti zodpovedajúcej deklarovanému predmetu podnikania, dotovanie produktov alebo služieb výrazne pod trhovými cenami alebo dokonca pod výrobnými nákladmi – čo samo osebe naznačuje, že skutočným zdrojom príjmov nie sú obchodné tržby, ale iné prostriedky – neprimeraný obrat vzhľadom na veľkosť a charakter podniku, absencia zamestnancov, fyzických priestorov alebo iných atribútov skutočnej podnikateľskej aktivity a prepojenie na jurisdikcie s nízkymi štandardmi transparentnosti. Pre finančné inštitúcie je identifikácia krycích podnikov jednou z najnáročnejších úloh hĺbkovej previerky, keďže sofistikované krycie podniky môžu mať reálnu webovú stránku, zamestnancov a zdanlivo legitímne obchodné vzťahy; kľúčom je porovnávanie deklarovanej obchodnej činnosti so skutočnými transakčnými tokmi, analýza ekonomickej logiky obchodného modelu a dôkladné preverenie skutočného vlastníka a jeho väzieb.

FUNDAMENTAL PRINCIPALS OF DOMESTIC LAW

Ide o základné právne zásady, na ktorých sú založené vnútroštátne právne systémy a ktoré poskytujú rámec, v ktorom sa tvoria vnútroštátne zákony a vykonávajú právomoci. Tieto základné zásady sú zvyčajne obsiahnuté alebo vyjadrené vo vnútroštátnej ústave alebo podobnom dokumente, alebo prostredníctvom rozhodnutí najvyššieho stupňa súdu, ktorý má právomoc záväzne vykladať alebo určovať vnútroštátne právo. Hoci sa to v jednotlivých krajinách líši, niektoré príklady takýchto základných zásad zahŕňajú práva na spravodlivý proces, prezumpciu neviny a právo osoby na účinnú súdnu ochranu.

FUNDS OR OTHER ASSETS

Pojem finančné prostriedky alebo iné aktíva znamená akékoľvek aktíva vrátane, ale nielen, finančných aktív, hospodárskych zdrojov (vrátane ropy a iných prírodných zdrojov), majetku každého druhu, hmotného alebo nehmotného, hnuteľného alebo nehnuteľného, nadobudnutého akýmkoľvek spôsobom, a právnych dokumentov alebo nástrojov v akejkoľvek forme vrátane elektronickej alebo digitálnej, ktoré preukazujú vlastnícke právo alebo podiel na ňom, takýchto finančných prostriedkov alebo iných aktív, okrem iného vrátane bankových úverov, cestovných šekov, bankových šekov, peňažných poukážok, akcií, cenných papierov, dlhopisov, zmeniek alebo akreditívov, ako aj akýchkoľvek úrokov, dividend alebo iných príjmov z týchto finančných prostriedkov alebo iných aktív alebo z nich plynúcich hodnôt a akýchkoľvek iných aktív, ktoré sa potenciálne môžu použiť na získanie finančných prostriedkov, tovaru alebo služieb.

V kontexte AML/CFT je zámerná šírka definície pojmu „finančné prostriedky“ základným predpokladom účinnosti celého sankčného a AML/CFT systému – úzka definícia obmedzená napríklad len na hotovosť alebo bankové vklady by páchateľom umožnila jednoducho obchádzať povinnosti prevodom hodnôt do iných foriem aktív. Práve preto medzinárodné sankčné režimy, odporúčania FATF aj smernice AMLD pracujú s najširším možným vymedzením pojmu, ktoré explicitne zahŕňa fyzickú hotovosť a bankové vklady, cenné papiere a investičné nástroje, nehnuteľnosti a hmotný majetok, pohľadávky a iné nehmotné aktíva, virtuálne aktíva a kryptomeny, drahé kovy, kamene a umelecké predmety a akékoľvek právne nároky na vyššie uvedené aktíva. Pre finančné inštitúcie má táto široká definícia priamy praktický dopad – zmrazenie finančných prostriedkov sankcionovaného subjektu sa nevzťahuje len na jeho bankové účty, ale na akékoľvek aktíva v správe alebo pod kontrolou inštitúcie, a povinnosť monitorovania a hlásenia sa rovnako vzťahuje na transakcie s akoukoľvek formou hodnoty, nielen na tradičné peňažné prevody.

FUZZY LOGIC

Technika porovnávania, ktorú používajú finančné inštitúcie na zvýšenie účinnosti procesov preverovania tým, že prekonávajú problémy, ako sú chybné záznamy a databázy. Fuzzy logika sa realizuje prostredníctvom algoritmov, ktoré používajú „stupne podobnosti“ na určenie pravdepodobnosti, že dve mená sú rovnaké. Fuzzy logika dokáže nájsť zhodu v nesprávne napísaných menách, neúplných menách a menách s rôznym pravopisom, ale podobnými zvukmi alebo fonetikou. Okrem toho fuzzy logika akceptuje rôzne formáty dátumu narodenia a iné nezrovnalosti. Hoci fuzzy logika zvyšuje pravdepodobnosť identifikácie potenciálnych cieľových zhôd, môže tiež zvýšiť počet falošne pozitívnych výsledkov.

GATEKEEPERS

Odborníci, ako sú právnici, notári, účtovníci, investiční poradcovia a poskytovatelia trustových a podnikových služieb, ktorí pomáhajú pri transakciách zahŕňajúcich pohyb peňazí a považujú sa za osoby, ktoré majú osobitnú úlohu pri identifikácii, prevencii a oznamovaní prania špinavých peňazí. Niektoré krajiny ukladajú na strážcov náležitej starostlivosti požiadavky, ktoré sú podobné požiadavkám na finančné inštitúcie.

V kontexte AML/CFT majú gatekeepers nezastupiteľné postavenie práve preto, že páchatelia prania špinavých peňazí a korupcie systematicky vyhľadávajú ich služby na legitímizáciu nelegálnych aktivít – právnik zakladajúci spoločnosť, notár overujúci prevod nehnuteľnosti, účtovník spravujúci finančné toky alebo poskytovateľ trustových služieb spravujúci majetok môžu nevedome alebo vedome poskytnúť rozhodujúci článok v reťazci prania špinavých peňazí. FATF vo svojich odporúčaniach (č. 22 a 23) explicitne zaraďuje gatekeepers medzi DNFBP a ukladá im povinnosti KYC/CDD, oznamovania podozrivých aktivít a uchovávania záznamov pri výkone špecifických činností. Osobitnou a dlhodobo kontroverznou otázkou je kolízia medzi AML/CFT oznamovacími povinnosťami a právnou profesijnou mlčanlivosťou (legal professional privilege) – väčšina jurisdikcií túto kolíziu rieši tak, že oznamovacia povinnosť sa nevzťahuje na informácie získané pri právnom zastupovaní klienta v súdnom konaní, avšak vzťahuje sa na všetky ostatné profesionálne činnosti vrátane zakladania spoločností, správy majetku a finančného poradenstva. Napriek formálnym regulačným požiadavkám zostáva dohľad nad gatekeepers vo väčšine jurisdikcií výrazne slabší ako dohľad nad finančnými inštitúciami, čo FATF opakovane identifikuje ako systémovú slabinu – práve nedostatočná regulácia a dohľad nad profesionálnymi sprostredkovateľmi umožňuje páchateľom využívať ich služby s relatívne nízkym rizikom odhalenia.

GLOBAL MAGNITSKY ACT

Legislatíva umožňujúca uvalenie sankcií (zákaz vstupu, zmrazenie majetku) na osoby zodpovedné za závažné porušenia ľudských práv a korupciu na celom svete. USA prijali Global Magnitsky Act v roku 2016, EÚ a ďalšie krajiny prijali podobné mechanizmy. Tieto sankcie sú súčasťou screeningových programov finančných inštitúcií.

GLOBAL PROGRAMME AGAINST MONEY LAUNDERING (GPML)

Globálny program proti praniu špinavých peňazí - kľúčový nástroj Úradu OSN pre kontrolu drog a prevenciu kriminality v boji proti praniu špinavých peňazí. Prostredníctvom GPML pomáha OSN členským štátom zavádzať právne predpisy proti praniu špinavých peňazí a pomáha im pri odhaľovaní, zaistení a konfiškácii nezákonných príjmov, ako to vyžadujú súvisiace nástroje OSN a celosvetovo uznávané normy, a to poskytovaním relevantnej a primeranej technickej pomoci na žiadosť štátov.

GLOBALIZATION

Globalizácia znamená integráciu národných hospodárskych, obchodných a komunikačných operácií podnikov zapojených do medzinárodného

obchodu. Globalizácia vo všeobecnosti zahŕňa rozšírenie národných perspektív na medzinárodné a vzájomne závislé perspektívy spoločnosti. Presadzuje voľnejší transfer tovarov a služieb, ako aj aktív cez národné a medzinárodné hranice. Predpokladá sa, že globalizácia môže obmedziť účinnosť sankcií, pretože globalizovaný trh umožňuje ľahšie nahradiť a presmerovať obchodné kanály.

GOVERNANCE

Riadenie je rozdelenie právomocí a rozhodovacích právomocí medzi predstavenstvom a manažmentom s cieľom zaviesť vnútorné kontroly na účely riadenia rizík a dodržiavania zákonov, predpisov a interných politík. Riadenie môže zahŕňať systémy kontroly a rovnováhy a zodpovednosť za vedenie a organizáciu.

V kontexte AML/CFT je kvalita riadenia považovaná za základný predpoklad účinnosti celého AML/CFT programu – regulátori a FATF pri hodnoteniach dôsledne skúmajú, či zodpovednosť za AML/CFT riziká je zakotvená na najvyššej úrovni riadenia inštitúcie, nielen na úrovni compliance funkcie. Tone from the top – postoj a angažovanosť predstavenstva a vrcholového manažmentu voči AML/CFT povinnostiam – je považovaný za jeden z najdôležitejších indikátorov skutočnej kultúry compliance v inštitúcii. Konkrétne požiadavky na governance v oblasti AML/CFT zahŕňajú jasnú zodpovednosť predstavenstva za schvaľovanie AML/CFT stratégie a rizikovej apetície, pravidelnú informovanosť predstavenstva o stave AML/CFT rizík a účinnosti programu, priamu prístupnosť MLRO alebo Compliance Officera k predstavenstvu bez filtrovania cez líniový manažment a zabezpečenie dostatočných zdrojov pre compliance funkciu ako prejav skutočného záväzku vedenia. Prípady závažných AML/CFT zlyhaní vo finančných inštitúciách opakovane ukázali, že ich koreňovou príčinou neboli nedostatky technických systémov, ale zlyhanie na úrovni riadenia – kultúra uprednostňujúca obchodné výsledky pred compliance, nedostatočný dohľad predstavenstva alebo zámerné ignorovanie varovných signálov zo strany vrcholového manažmentu.

GRANTOR

Strana, ktorá prevádza vlastnícke právo alebo vlastníctvo majetku alebo aktív. V prípade trustu je to zvyčajne osoba, ktorá trust vytvára alebo financuje.

GREYLIST

Greylist je zoznam subjektov, ktoré sú podozrivé alebo u ktorých je vyššie riziko, že spôsobia negatívny vplyv na firmu. V kontexte sankcií greylist obsahuje názvy krajín so strategickými nedostatkami v režimoch boja proti praniu špinavých peňazí a financovaniu terorizmu. Okrem toho tieto krajiny tiež nedosiahli dostatočný pokrok alebo sa inak nezaviazali k akčným plánom na odstránenie nedostatkov zistených FATF.

GULF COOPERATION COUNCIL (GCC)

GCC vznikla v roku 1981 a podporuje spoluprácu medzi svojimi členskými štátmi v oblasti hospodárstva a priemyslu. Medzi členské štáty patria Kuvajt, Bahrajn, Katar, Saudská Arábia, Omán a Spojené arabské emiráty. GCC je členom FATF, hoci jej jednotliví členovia nie sú členmi.

HAWALA

Od teroristických útokov na Spojené štáty z 11. septembra 2001 sa zvýšil záujem verejnosti o neformálne systémy prevodu peňazí po celom svete, najmä o systém hawala. Dôvodom je údajná úloha systému hawala pri financovaní nezákonných a teroristických aktivít, ako aj jeho tradičná úloha prevodu peňazí medzi jednotlivcami a rodinami, často v rôznych krajinách. V tejto súvislosti sa vlády a medzinárodné orgány snažia lepšie pochopiť tieto systémy, posúdiť ich ekonomické a regulačné dôsledky a navrhnúť najvhodnejší prístup na ich riešenie.

Neformálne systémy prevodu finančných prostriedkov (IFT) sa používajú v mnohých regiónoch na prevod finančných prostriedkov na vnútroštátnej aj medzinárodnej úrovni. Systém hawala je jedným zo systémov IFT, ktoré existujú pod rôznymi názvami v rôznych regiónoch sveta. Je však dôležité rozlišovať systém hawala od pojmu hawala, ktorý v arabskom bankovom žargóne znamená „prevod“ alebo „telegram“. Systém hawala označuje neformálny kanál na prevod finančných prostriedkov z jedného miesta na druhé prostredníctvom poskytovateľov služieb - známych ako hawaladári - bez ohľadu na povahu transakcie a zúčastnené krajiny. Hoci transakcie hawala väčšinou iniciujú emigrujúci pracovníci žijúci v rozvinutej krajine, systém hawala možno použiť aj na posielanie finančných prostriedkov z rozvojovej krajiny, hoci účel prevodu finančných prostriedkov je zvyčajne iný

HAWALADA/HAWALADAR

Sprostredkovateľ hawala.

HIT

Potenciálna zhoda alebo zhoda mena počas procesu kontroly sankcií, ktorá naznačuje možnú sankcionovanú osobu.

HUMAN RIGHTS

Základné práva človeka, ktoré sú „vlastné všetkým ľuďom bez ohľadu na rasu, pohlavie, národnosť, etnický pôvod, jazyk, náboženstvo alebo iné postavenie“. Ľudské práva sú vládou považované za nezrušiteľné. Všeobecná deklarácia ľudských práv OSN bola prijatá v roku 1948 s cieľom chrániť sociálne, kultúrne, finančné a politické práva jednotlivcov. Medzi ľudské práva, na ktoré sa deklarácia vzťahuje, patrí právo na život, slobodu, vzdelanie a rovnosť pred zákonom. Deklarácia tiež stanovuje ochranu človeka, ktorá je základom mnohých moderných národných ústav, ako napríklad sloboda zhromažďovania a právo na slobodu prejavu, náboženské slobody a iné slobody. Žiadna krajina nie je povinná dodržiavať normy ľudských práv, napriek tomu tieto normy slúžia ako vodítko pre nezávislosť, záujem a ochranu človeka.

HUMAN SMUGGLING

Pašovanie ľudí znamená prepravu alebo nelegálny vstup osôb cez medzinárodné hranice v rozpore so zákonmi jednej alebo viacerých krajín. Pašovanie ľudí sa od obchodovania s ľuďmi líši tým, že sa zameriava skôr na vstup alebo prepravu než na vykorisťovanie dotknutej osoby.

HUMAN TRAFFICKING

Známe aj ako obchodovanie s ľuďmi. Obchodovanie s ľuďmi, najčastejšie na účely sexuálneho otroctva, nútenej práce alebo komerčného sexuálneho vykorisťovania. Obchodovanie s ľuďmi sa vyskytuje takmer vo všetkých krajinách sveta a často sa uvádza ako druhý najväčší zločinecký podnik na svete.

IDENTIFIER

Typ informácií o cieli sankcií, ktoré sú zaznamenané na sankčnom zozname, napríklad meno, dátum narodenia, jurisdikcia, národné identifikačné číslo, subjekt, s ktorým je cieľ spojený, informácie o sankciách uložených voči cieľu, registrovaná právna adresa a webová adresa. Identifikátory sa vzťahujú na fyzické aj právnické osoby.

IDENTIFICATION DATA

Pojem identifikačné údaje sa vzťahuje na spoľahlivé, nezávislé zdrojové dokumenty, údaje alebo informácie o totožnosti fyzickej alebo právnickej osoby. Zahŕňajú doklady totožnosti vydané štátom, obchodné registre, výpisy z verejných databáz a iné dôveryhodné zdroje.

V kontexte AML/CFT sú identifikačné údaje základným stavebným kameňom celého procesu KYC/CDD – kvalita, spoľahlivosť a aktuálnosť identifikačných údajov priamo určuje, do akej miery môže inštitúcia dôverovať svojej znalosti klienta a hodnoteniu jeho rizikového profilu. Kľúčovým slovom je „spoľahlivé a nezávislé" – inštitúcie sú povinné overovať identifikačné údaje z nezávislých zdrojov a nemôžu sa spoliehať výlučne na informácie poskytnuté samotným klientom, keďže práve falošná alebo zavádzajúca identifikácia je prvým krokom pri zneužívaní finančného systému na pranie špinavých peňazí. Regulačné požiadavky na identifikačné údaje sa neustále vyvíjajú – digitalizácia a rozvoj elektronickej identifikácie (eID) prinášajú nové možnosti overenia totožnosti na diaľku, pričom nariadenie eIDAS v EÚ a usmernenia EBA k digitálnej identite stanovujú podmienky, za ktorých môžu inštitúcie akceptovať elektronické identifikačné prostriedky ako rovnocenné fyzickým dokladom totožnosti. Osobitnou výzvou zostáva overovanie identifikačných údajov pri klientoch z jurisdikcií s nedostatočnou infraštruktúrou evidencie obyvateľstva, kde spoľahlivé štátom vydané doklady totožnosti nemusia byť dostupné pre všetkých klientov.

IDENTITY THEFT

Krádež totožnosti je proces, ktorý zločinci používajú na získanie osobných a finančných informácií jednotlivca bez jeho súhlasu. Robí sa to s cieľom vykonávať neoprávnené transakcie alebo trestnú činnosť.

INTERGOVERNMENTAL ACTION GROUP AGAINST MONEY-LAUNDERING IN WEST AFRICA (GIABA)

GIABA bola založená 10. decembra 1999 rozhodnutím orgánu hláv štátov a vlád ECOWAS. Mandát GIABA bol revidovaný v januári 2006 s cieľom plne začleniť a náležite zohľadniť nevyhnutnosť boja proti financovaniu terorizmu. Členovia GIABA uznávajú, že pranie špinavých peňazí a financovanie terorizmu sú pre svetové spoločenstvo mimoriadne dôležité otázky, ktoré si vyžadujú globálne opatrenia. Ďalej, že ekonomiky a finančné systémy krajín je potrebné chrániť pred praním špinavých peňazí a výnosov z teroristických aktivít. Členovia GIABA uznávajú, že západná Afrika sa musí zaoberať týmito problémami a nájsť ich globálne riešenia. GIABA sa stala pridruženým členom FATF v júni 2010.

INTERMEDIARY FINANCIAL INSTITUTION

Vzťahuje sa na finančnú inštitúciu v reťazci sériových alebo krycích platieb, ktorá prijíma a odosiela prevod v mene finančnej inštitúcie príkazcu a finančnej inštitúcie príjemcu alebo inej sprostredkujúcej finančnej inštitúcie (ako sa tento pojem používa vo výkladovej poznámke k odporúčaniu FATF 16).

INTERNATIONAL MONEY LAUNDERING INFORMATION NETWORK (IMOLIN)

Medzinárodná informačná sieť o praní špinavých peňazí - internetová sieť, ktorá pomáha vládam, organizáciám a jednotlivcom v boji proti praniu špinavých peňazí a financovaniu terorizmu. IMOLIN bola vytvorená v spolupráci s poprednými svetovými organizáciami na boj proti praniu špinavých peňazí.

INTERNATIONAL MONETARY FUND (IMF)

MMF bol založený v roku 1944 po veľkej hospodárskej kríze v 30. rokoch 20. storočia. Snahou 44 zakladajúcich členských krajín bolo vytvoriť rámec pre medzinárodnú hospodársku spoluprácu. Dnes je jeho členom 190 krajín a jeho zamestnanci pochádzajú zo 150 krajín. MMF je riadený a zodpovedný týmto 190 krajinám, ktoré tvoria jeho takmer celosvetové členstvo. Cieľom je podporovať globálnu menovú spoluprácu, zabezpečovať finančnú stabilitu, uľahčovať medzinárodný obchod, podporovať vysokú zamestnanosť a udržateľný hospodársky rast a znižovať chudobu na celom svete. Ciele organizácie sa od jej založenia nezmenili. Jeho operácie, ktoré zahŕňajú dohľad, finančnú pomoc a technickú podporu, sa prispôsobili meniacim sa potrebám členských krajín.

INTERNATIONAL ORGANIZATIONS

Medzinárodné organizácie sú subjekty zriadené formálnymi politickými dohodami medzi ich členskými štátmi, ktoré majú štatút medzinárodných zmlúv; ich existencia je uznaná zákonom v ich členských krajinách; a nepovažujú sa za rezidentské inštitucionálne jednotky krajín, v ktorých sa nachádzajú. Príkladmi medzinárodných organizácií sú Organizácia Spojených národov a pridružené medzinárodné organizácie, ako napríklad Medzinárodná námorná organizácia; regionálne medzinárodné organizácie, ako napríklad Rada Európy, inštitúcie Európskej únie, Organizácia pre bezpečnosť a spoluprácu v Európe a Organizácia amerických štátov; vojenské medzinárodné organizácie, ako napríklad Organizácia Severoatlantickej zmluvy, a hospodárske organizácie, ako napríklad Svetová obchodná organizácia alebo Združenie národov juhovýchodnej Ázie atď.

INEQUALITIES LIST

Zoznam slov alebo mien, ktoré automatizované nástroje na preverovanie často mylne považujú za zhodné, a tým vytvárajú potenciálne zhody s cieľmi uvedenými na sankčných zoznamoch. Ide o slová alebo mená, ktoré tím organizácie pre dodržiavanie predpisov skontroloval a potvrdil, že sa v skutočnosti nezhodujú, napríklad Andrew a Andrea. Pridanie do zoznamu nerovností uplatní nerovnosť na všetky budúce prípady skríningu a zníži pravdepodobnosť budúcej zhody. Zoznamy nerovností by preto mali mať dostatočné kontrolné mechanizmy (aspoň dvojnásobné kontroly) na pridávanie do zoznamu a pravidelnú kontrolu.

INHERENT RISK

Úroveň sankčných rizík, ktorá existuje pred uplatnením kontrol na ich zmiernenie. Existujú štyri hlavné kategórie inherentných rizík: zákazníci, produkty a služby, krajiny a dodávateľské kanály. Inherentné riziko je spojené s procesom hodnotenia rizík, ktorý hodnotí účinnosť kontrolných mechanizmov inštitúcie. Prirodzené riziko zohľadňuje pravdepodobnosť a vplyv nedodržania pravidiel pred zvážením akýchkoľvek zmierňujúcich účinkov procesov riadenia rizík.

V kontexte AML/CFT tvorí hodnotenie inherentného rizika prvý a nevyhnutný krok celého procesu hodnotenia rizík podľa prístupu založeného na riziku – bez pochopenia prirodzenej rizikovosti vlastného obchodného modelu, klientskej základne a produktového portfólia nie je možné navrhnúť primerané a účinné kontrolné mechanizmy. Výsledné reziduálne riziko (residual risk) vzniká ako rozdiel medzi inherentným rizikom a účinnosťou zavedených kontrol – práve toto reziduálne riziko by malo byť v súlade s rizikovou apetíciou inštitúcie schválenou predstavenstvom. Regulátori pri dohľadových inšpekciách posudzujú, či inštitúcia správne identifikovala a ohodnotila svoje inherentné riziká v každej z uvedených kategórií – podhodnotenie inherentného rizika vedie k nedostatočným kontrolám a systémovým zraniteľnostiam, zatiaľ čo jeho nadhodnotenie vedie k neprimeranému zaťaženiu klientov a operačnej neefektívnosti. Osobitnou výzvou je dynamická povaha inherentného rizika – vstup do nového produktového segmentu, expanzia do novej geografickej oblasti alebo zmena klientskej základne môžu zásadne zmeniť rizikový profil inštitúcie a vyžadujú bezodkladné prehodnotenie celkového hodnotenia rizík.

INTEGRATION

Fáza integrácie, ktorá sa často označuje ako tretia a posledná fáza klasického procesu prania špinavých peňazí, umiestňuje vyprané finančné prostriedky späť do ekonomiky tým, že ich opätovne vkladá do finančného systému a dáva im zdanie legálnosti. Po úspešnej integrácii sú nelegálne prostriedky fakticky nerozoznateľné od legitímne nadobudnutého majetku.

V kontexte AML/CFT predstavuje integrácia fázu, v ktorej je pranie špinavých peňazí najťažšie odhaliteľné – na rozdiel od fázy umiestnenia (placement), kde je riziko odhalenia najvyššie práve pre priamy kontakt nelegálnej hotovosti s finančným systémom, v štádiu integrácie sú prostriedky už niekoľkonásobne transformované a vzdialené od svojho pôvodu. Typické techniky integrácie zahŕňajú investície do nehnuteľností s následným predajom za trhovú cenu generujúcim zdanlivo legitímny príjem, nákup luxusných aktív – umeleckých diel, drahých kovov, jácht alebo luxusných vozidiel – a ich následný predaj, zakladanie alebo akvizíciu legitímnych podnikov financovaných vypranými prostriedkami, fiktívne pôžičky, pri ktorých sankcionovaná alebo kriminálna strana požičia sebe samej vyprané prostriedky a splácanie týchto pôžičiek slúži ako legitímny zdroj príjmu, a využívanie komplexných investičných štruktúr zahŕňajúcich offshore fondy, trusty a holdingové spoločnosti na konečné začlenenie prostriedkov do legálnej ekonomiky. Pre finančné inštitúcie je identifikácia integrácie obzvlášť náročná, keďže jednotlivé transakcie v tejto fáze môžu vyzerať úplne legitímne – účinná ochrana si vyžaduje komplexné hodnotenie celkového vzorca správania klienta, pôvodu jeho majetku a konzistentnosti jeho finančných aktivít s deklarovaným obchodným profilom, nie len posudzovanie individuálnych transakcií v izolácii.

INTERNAL EVASION

Situácia, keď vlastný zamestnanec finančnej inštitúcie vedome pácha sankčné porušenie alebo ho aktívne uľahčuje – buď neuplatňovaním alebo zámerným obchádzaním vnútorných kontrolných mechanizmov, manipuláciou s transakčnými monitorovacími systémami, alebo zneužívaním klientskych účtov na zatajenie pôvodu finančných prostriedkov. dopustí porušenia sankcií alebo ho uľahčí. Príklady zahŕňajú nasledujúce: keď zamestnanec buď neuplatňuje, alebo prekonáva vnútorné kontroly s cieľom obísť nástroje na monitorovanie transakcií alebo keď zamestnanec používa klientske účty na utajenie pôvodu finančných prostriedkov.

V kontexte AML/CFT predstavuje interné obchádzanie sankcií najzávažnejšiu formu sankčného porušenia, keďže útočí priamo na integritu vnútorného kontrolného systému inštitúcie zvnútra – zamestnanec s prístupom k systémom, procesným znalostiam a dôverou vedenia je schopný obchádzať kontrolné mechanizmy spôsobom, ktorý je oveľa ťažšie odhaliteľný ako externé pokusy o obchádzanie sankcií. Regulátori pri hodnotení prípadov interného obchádzania posudzujú nielen samotné konanie zamestnanca, ale aj systémové podmienky, ktoré ho umožnili – nedostatočné oddelenie právomocí, absenciu princípu štyroch očí pri kritických rozhodnutiach, nedostatočný interný audit alebo kultúru, v ktorej sa na varovné signály nereagovalo. Účinná prevencia interného obchádzania sankcií vyžaduje kombináciu personálnych opatrení – previerky zamestnancov pri nástupe aj priebežne, jasné etické štandardy a whistleblowing mechanizmy – technických kontrol zahŕňajúcich automatické logovanie systémových aktivít, obmedzenie prístupu k citlivým funkciám a pravidelný audit override akcií, a kultúrnych prvkov spočívajúcich v nastavení prostredia, kde zamestnanci aktívne hlásia podozrenia bez strachu z odvetných opatrení. Prípady interného obchádzania sankcií vedú spravidla k najprísnejším regulačným sankciám voči inštitúcii, keďže preukazujú fundamentálne zlyhanie kultúry compliance na všetkých úrovniach riadenia.

INTERNATIONAL BUSINESS COMPANY (IBC)

Rôzne offshore podnikové štruktúry, ktoré sú určené na podnikanie mimo jurisdikcie, v ktorej sú založené, a vyznačujú sa rýchlym založením, utajením, širokými právomocami, nízkymi nákladmi, nízkym až nulovým zdanením a minimálnymi požiadavkami na podávanie správ a hlásení.

INVESTIGATION

Proces získavania, vyhodnocovania, zaznamenávania a uchovávania informácií o fyzickej alebo právnickej osobe, s ktorou sa obchoduje, v reakcii na upozornenie naznačujúce možné porušenie sankcií. Vyšetrovanie sa často začína jednoduchými kontrolami, než sa prejde k ďalšiemu vyšetrovaniu, ako je preskúmanie účtu, oslovenie klienta a prípadná eskalácia na funkciu dodržiavania predpisov.

INTERNATIONAL ORGANISATION OF SECURITIES COMMISSIONS (IOSCO)

Medzinárodná organizácia komisií pre cenné papiere (IOSCO) je medzinárodný orgán, ktorý združuje svetové regulačné orgány pre cenné papiere a je uznávaný ako globálny tvorca noriem pre sektor cenných papierov. IOSCO vyvíja, implementuje a podporuje dodržiavanie medzinárodne uznávaných štandardov pre reguláciu cenných papierov. Intenzívne spolupracuje so skupinou G20 a Radou pre finančnú stabilitu (FSB) na globálnom programe regulačných reforiem. IOSCO bola založená v roku 1983. Jej členovia regulujú viac ako 95 % svetových trhov s cennými papiermi vo viac ako 130 jurisdikciách, regulátori cenných papierov na rozvíjajúcich sa trhoch tvoria 75 % jej riadnych členov.

ISOLATION COMPANY

Spoločnosť, ktorá pomáha osobám, ktoré sa vyhýbajú sankciám, vyhnúť sa dojmu, že sú zapojené do sankcií, alebo subjektom, ktoré sa snažia obchodovať so subjektom, na ktorý sa sankcie vzťahujú. Vyhýbajúce sa subjekty si vyberajú izolačnú spoločnosť buď pre jej minulé obchodné aktivity, alebo pre jej nedostatočne vysledovateľné spojenie so subjektmi zapojenými do vyhýbajúcej sa činnosti.

JOINT COMPREHENSIVE PLAN OF ACTION (JCPOA)

Podrobná dohoda s piatimi prílohami, ktorú Irán a P5+1 (Čína, Francúzsko, Nemecko, Rusko, Spojené kráľovstvo a Spojené štáty) dosiahli 14. júla 2015. Jadrová dohoda bola schválená rezolúciou Bezpečnostnej rady OSN č. 2231 prijatou 20. júla 2015. Dodržiavanie ustanovení JCPOA týkajúcich sa jadrového programu zo strany Iránu overuje Medzinárodná agentúra pre atómovú energiu (MAAE) podľa určitých požiadaviek stanovených v dohode. Prezident Trump 8. mája 2018 oznámil, že Spojené štáty odstúpia od JCPOA a obnovia jadrové sankcie USA voči iránskemu režimu. Od roku 2021 prebiehali rokovania o obnovení dohody pod vedením prezidenta Bidena, avšak v roku 2022-2023 sa rokovania definitívne zrútili. JCPOA je od roku 2023 prakticky nefunkčný – Irán výrazne rozšíril jadrový program.

JURISDICTION OF CITIZENSHIP

Krajina (alebo krajiny, v prípade dvojakého občianstva), ktorej je osoba legálnym občanom.

JURISDICTION OF RESIDENCE

Krajina, v ktorej sa jednotlivec zdržiava väčšinu času; krajina, v ktorej má jednotlivec svoje hlavné bydlisko.

KLEPTOCRAT

Skorumpovaný vodca, ktorý využíva ľudí a zdroje štátu na osobný prospech.

KNOW YOUR BUSINESS (KYB)

Proces overovania totožnosti a hodnotenia rizika právnických osôb (podnikov), analogický k procesu KYC pre fyzické osoby. KYB zahŕňa overenie právneho statusu, vlastníckej štruktúry, skutočného vlastníctva a povahy obchodnej činnosti zákazníka. Je nevyhnutnou súčasťou hĺbkovej previerky zákazníka (CDD) pri nadväzovaní obchodných vzťahov s právnickými osobami.

V kontexte AML/CFT je KYB komplexnejší a náročnejší proces ako KYC pre fyzické osoby, keďže právnické osoby môžu mať mnohovrstevnaté

vlastnícke štruktúry prechádzajúce viacerými jurisdikciami, ktoré sú zámerné navrhnuté na zatajenie skutočného vlastníka. Efektívny KYB proces musí preniknúť cez všetky vrstvy vlastníckej štruktúry až k fyzickej osobe, ktorá v konečnom dôsledku vlastní alebo kontroluje daný subjekt, overiť konzistentnosť deklarovanej obchodnej činnosti so skutočnými transakčnými tokmi a posúdiť, či obchodný model a vlastnícka štruktúra majú legitímny ekonomický zmysel alebo slúžia primárne na zakrytie skutočného vlastníka a pôvodu prostriedkov. Osobitnou výzvou KYB sú trusty, nadácie a iné právne zriadenia, pri ktorých identifikácia skutočného vlastníka vyžaduje analýzu zriaďovacích dokumentov, identifikáciu zakladateľa, správcov a skutočných beneficientov. Zavedenie registrov skutočných vlastníkov v EÚ na základe smerníc AMLD síce výrazne uľahčilo KYB proces, avšak spoľahlivosť a úplnosť týchto registrov sa medzi členskými štátmi výrazne líši, čo znamená, že registre musia byť jedným zo zdrojov overenia, nie jediným.

KNOWLEDGE

Psychický stav sprevádzajúci zakázaný čin. Vo výkladových poznámkach k odporúčaniu 3 40 odporúčaní FATF z roku 2012 sa uvádza, že krajiny by mali zabezpečiť, aby úmysel a vedomosti potrebné na preukázanie trestného činu prania špinavých peňazí boli v súlade so štandardmi stanovenými vo Viedenskom a Palermskom dohovore vrátane koncepcie, že takýto duševný stav možno odvodiť z objektívnych skutkových okolností. Presná definícia vedomostí, ktoré sprevádzajú zákon proti praniu špinavých peňazí, sa v jednotlivých krajinách líši. Za vedomosť možno za určitých okolností považovať aj úmyselnú slepotu; to znamená „úmyselné vyhýbanie sa poznaniu skutočnosti“, ako tento pojem definovali niektoré súdy.

KNOW YOUR CUSTOMER (KYC)

Zásady a postupy proti praniu špinavých peňazí používané na určenie skutočnej totožnosti klienta a typu činnosti, ktorá je „bežná a očakávaná“, a na odhalenie činnosti, ktorá je pre konkrétneho klienta „neobvyklá“.

V kontexte AML/CFT je KYC ústredným pilierom celého systému predchádzania praniu špinavých peňazí – bez dostatočnej znalosti klienta nie je možné ani zmysluplné monitorovanie transakcií, ani hodnotenie rizík, ani podávanie kvalitných oznámení o podozrivých aktivitách. KYC nie je jednorazový proces pri otvorení účtu, ale kontinuálna povinnosť pozostávajúca z niekoľkých vzájomne previazaných prvkov. Identifikácia a overenie totožnosti zahŕňa získanie a overenie základných identifikačných údajov z nezávislých a spoľahlivých zdrojov – pri fyzických osobách meno, dátum narodenia, adresa a doklad totožnosti, pri právnických osobách obchodné meno, sídlo, právna forma, vlastnícka štruktúra a identifikácia skutočného vlastníka. Pochopenie obchodného vzťahu si vyžaduje zistiť účel a zamýšľanú povahu vzťahu, zdroj finančných prostriedkov a majetku a očakávaný objem a charakter transakcií. Rizikové profilovanie na základe získaných informácií určuje, aká úroveň hĺbkovej previerky je primeraná – štandardná CDD, zjednodušená SDD alebo rozšírená EDD. Priebežná aktualizácia zabezpečuje, že informácie o klientovi zostávajú aktuálne a relevantné počas celého trvania obchodného vzťahu. Kvalita KYC programu je jedným z najdôležitejších ukazovateľov posudzovaných pri dohľadových inšpekciách – regulátori osobitne skúmajú, či inštitúcie skutočne rozumejú svojim klientom a ich obchodným aktivitám, alebo len formálne zbierajú dokumenty bez skutočného pochopenia rizík, ktoré ich klienti predstavujú.

KNOW YOUR EMPLOYEE (KYE)

Politiky a postupy proti praniu špinavých peňazí na získanie lepších znalostí a pochopenia zamestnancov inštitúcie na účely odhaľovania konfliktov záujmov, prania špinavých peňazí, trestnej činnosti v minulosti a podozrivých činností.

V kontexte AML/CFT je KYE priamou reakciou na riziko interného obchádzania sankcií a interných hrozieb všeobecne – zamestnanec s prístupom k systémom, procesným znalostiam a dôverou vedenia predstavuje osobitné riziko, ktoré nemôžu eliminovať technické kontroly samy osebe. Efektívny KYE program zahŕňa previerky pred nástupom do zamestnania overujúce trestnú minulosť, finančnú spoľahlivosť a pravdivosť údajov v životopise, priebežné monitorovanie správania zamestnancov vrátane sledovania systémových aktivít, detekcie neobvyklých prístupov k citlivým údajom a vyhodnocovania zmien v životnom štýle nezodpovedajúcich príjmom, pravidelnú aktualizáciu previerok pri zmene pracovného zaradenia alebo prístupu k citlivým systémom, jasné mechanizmy na hlásenie podozrivého správania kolegov vrátane anonymného whistleblowingu a kultúru, v ktorej je etické správanie aktívne oceňované a porušenia sú dôsledne riešené. Regulátori pri dohľadových inšpekciách posudzujú KYE ako integrálnu súčasť celkového AML/CFT programu – nedostatočná znalosť vlastných zamestnancov a absencia mechanizmov na detekciu interných hrozieb je považovaná za závažnú systémovú slabinu, ktorá môže zmariť aj inak dobre navrhnutý AML/CFT program, čo potvrdzujú viaceré historické prípady, v ktorých kľúčovú úlohu pri rozsiahlom praní špinavých peňazí zohrali práve insideri s privilegovaným prístupom k systémom a procesným znalostiam inštitúcie.

LAW

V odporúčaniach FATF 10, 11 a 20 sa pojem „zákon“ vzťahuje na akýkoľvek právny predpis vydaný alebo schválený v parlamentnom procese alebo iným rovnocenným spôsobom ustanoveným v ústavnom rámci krajiny, ktorý ukladá záväzné požiadavky so sankciami za ich nedodržanie. Sankcie za ich nedodržanie by mali byť účinné, primerané a odrádzajúce (pozri odporúčanie 35). Pojem zákon zahŕňa aj súdne rozhodnutia, ktoré ukladajú príslušné požiadavky a ktoré sú záväzné a autoritatívne vo všetkých častiach krajiny (ako sa tento pojem používa v poznámke o právnom základe požiadaviek na finančné inštitúcie a DNFBP).

LAYERING (VRSTVENIE)

Druhá fáza klasického trojstupňového procesu prania špinavých peňazí medzi umiestnením a integráciou, vrstvenie, zahŕňa vzdialenie nezákonných príjmov od ich zdroja vytvorením zložitých úrovní finančných transakcií navrhnutých tak, aby zamaskovali auditnú stopu a zabezpečili anonymitu. Vrstenie spočíva v zámernom vzďaľovaní nelegálnych prostriedkov od ich pôvodného zdroja prostredníctvom série komplexných finančných transakcií navrhnutých tak, aby zničili auditovateľnú stopu, zakryli pôvod prostriedkov a zabezpečili anonymitu skutočného vlastníka.

V kontexte AML/CFT predstavuje vrstenie fázu, v ktorej páchatelia vyvíjajú najväčšiu kreativitu a sofistikovanosť – cieľom je vytvoriť toľko vrstiev transakcií, jurisdikcií a právnych štruktúr, aby bolo pre orgány činné v trestnom konaní prakticky nemožné sledovať pôvod prostriedkov. Typické techniky vrstenia zahŕňajú sériu rýchlych medzibankových prevodov prechádzajúcich cez viaceré jurisdikcie s rôznymi štandardmi AML/CFT, konverziu prostriedkov medzi rôznymi menami, aktívami a finančnými nástrojmi s cieľom prerušiť sledovateľnosť, využívanie shell companies, trustov a nominálnych vlastníkov v offshore jurisdikciách na vytvorenie nepriehľadných vlastníckych štruktúr, nákup a predaj nehnuteľností, umeleckých diel alebo luxusných aktív ako prostredníkov na transformáciu formy majetku, využívanie korešpondenčného bankovníctva na presun prostriedkov cez reťazec bánk bez priameho vzťahu s pôvodným klientom a v súčasnosti čoraz rozšírenejšie využívanie virtuálnych aktív, mixérov a DeFi protokolov, ktoré umožňujú mimoriadne rýchle a ťažko sledovateľné vrstenie v celosvetovom meradle. Pre finančné inštitúcie je identifikácia vrstenia náročná práve preto, že jednotlivé transakcie môžu vyzerať legitímne – odhalenie vrstenia si vyžaduje schopnosť analyzovať vzorce naprieč viacerými transakciami, účtami a časovými obdobiami, a nie len posudzovať izolované transakcie; práve preto moderné systémy transaction monitoringu prechádzajú od pravidlami riadených prístupov k analytike správania a detekcii sietí (network analysis), ktoré sú schopné identifikovať koordinované vzorce typické pre vrstenie aj naprieč zdanlivo nesúvisiacimi účtami a subjektmi.

LEGAL ARRANGEMENT

Právna štruktúra umožňujúca oddelenie formálneho vlastníctva od skutočného ekonomického prospechu z majetku. Zahŕňa predovšetkým výslovné trusty a im podobné zriadenia uznávané v rôznych právnych systémoch - fiducie vo frankofónnych jurisdikciách, Treuhand v nemecky hovoriacich krajinách, fideicomiso v latinskoamerických jurisdikciách a ďalšie ekvivalentné štruktúry.

V kontexte AML/CFT predstavujú právne zriadenia osobitne rizikovú kategóriu, keďže ich základnou charakteristikou je práve oddelenie formálneho vlastníctva od skutočného ekonomického prospechu – čo je presne ten efekt, ktorý páchatelia prania špinavých peňazí, korupcie a daňových únikov aktívne vyhľadávajú. Správca trustu (trustee) je síce formálnym vlastníkom majetku, avšak skutočný ekonomický prospech plynie beneficientom, ktorých totožnosť nemusí byť verejne známa. FATF odporúčanie č. 25 explicitne vyžaduje, aby krajiny zabezpečili transparentnosť právnych zriadení a dostupnosť informácií o ich zakladateľoch, správcoch, beneficientoch a majetku príslušným orgánom, pričom revízia tohto odporúčania v roku 2022 tieto požiadavky výrazne sprísnila. Pre finančné inštitúcie poskytujúce služby trustom a iným právnym zriadeniam vyplývajú osobitné KYB povinnosti zahŕňajúce identifikáciu zakladateľa (settlor/grantor), všetkých správcov (trustees), protektora trustu ak existuje, všetkých beneficientov alebo tried beneficientov a akejkoľvek inej osoby vykonávajúcej skutočnú kontrolu nad trustom; komplexnosť a cezhraničný charakter mnohých trustových štruktúr pritom predstavuje jednu z najnáročnejších praktických výziev v oblasti identifikácie skutočného vlastníka.

LEGAL RISK

Definované v dokumente Bazilejská previerka klienta pre banky z roku 2001 ako možnosť, že súdne spory, nepriaznivé rozsudky alebo zmluvy, ktoré nemožno vymáhať, môžu narušiť alebo poškodiť finančnú inštitúciu. Okrem toho môžu banky utrpieť administratívne alebo trestnoprávne sankcie uložené vládou. Súdny spor týkajúci sa banky môže mať pre inštitúciu závažnejšie dôsledky než len právne náklady. Banky sa nebudú schopné účinne chrániť pred takýmito právnymi rizikami, ak nebudú uplatňovať náležitú starostlivosť pri identifikácii klientov a pochopení a riadení ich vystavenia riziku prania špinavých peňazí.

LETTER OF CREDIT

Úverový nástroj vydaný bankou, ktorý zaručuje platby v mene klienta tretej strane, ak sú splnené určité podmienky.

LICENSE

Písomné povolenie vydané orgánom dohľadu nad sankciami, ktoré povoľuje činnosť, ktorá by inak mohla byť zakázaná alebo obmedzená na základe konkrétnej sankcie. Zákony alebo nariadenia prijaté na vykonávanie finančných sankcií vo všeobecnosti obsahujú formulácie, ktoré umožňujú uskutočnenie inak zakázaných transakcií za určitých okolností, či už prostredníctvom všeobecného alebo osobitného povolenia. Všeobecná licencia je výnimka, na základe ktorej môžu vykonávať transakcie všetky osoby - príkladom môže byť transakcia na účely humanitárnej pomoci. Osobitná licencia je výnimkou pre žiadateľa o licenciu a stanovuje okolnosti, za ktorých môže žiadateľ vykonávať transakcie, ak mu bude licencia udelená.

LIMITED LIABILITY COMPANY (LLC)

Špecificky vymedzený typ podnikania v Spojených štátoch, v ktorom je osobná zodpovednosť oddelená od zodpovednosti právnických osôb. LLC sú obzvlášť obľúbené vo vysoko rizikových podnikoch, pretože jednotlivci (vlastníci, riaditelia atď.), ktorí sú s takýmito podnikmi spojení, sa snažia vyhnúť osobnej zodpovednosti za podnikové dlhy alebo súdne spory.

LOOK-BACK (OR LOOK-BACK REVIEW)

Proces spätného pohľadu na transakčnú aktivitu zákazníka za určité časové obdobie v minulosti. Spätné preskúmanie minulých transakcií môže pomôcť overiť skutočnú aktivitu klienta a poskytnúť „červené vlajky“ identifikovaním transakcií, ktoré by mohli naznačovať prepojenie s cieľmi sankcií, jurisdikciami alebo obmedzeniami.

MANDATORY SANCTIONS LISTS

Nadnárodné sankčné zoznamy, napríklad zoznamy zahŕňajúce ciele určené rezolúciami Bezpečnostnej rady OSN (BR OSN), ktoré sa musia preveriť. V závislosti od krajiny, v ktorej sa podnik nachádza a pôsobí, sa môžu vyžadovať (t. j. sú povinné) miestne sankčné režimy, ktoré by bolo potrebné zahrnúť do programu firmy na dodržiavanie sankcií.

MEMORANDUM OF UNDERSTANDING (MOU)

Dohoda medzi dvoma stranami, ktorá stanovuje súbor zásad, ktorými sa riadi ich vzťah v určitej záležitosti. Memorandum o porozumení často používajú krajiny na úpravu spoločného využívania majetku v medzinárodných prípadoch zabavenia majetku alebo na stanovenie svojich povinností v rámci iniciatív proti praniu špinavých peňazí. Finančné spravodajské jednotky (FIU), ktorých úlohou je priebežne prijímať a analyzovať správy o podozrivých transakciách a udržiavať úzke väzby s policajnými a colnými orgánmi, si v rámci vyšetrovania medzi sebou neformálne vymieňajú informácie, zvyčajne na základe memoranda o porozumení.

MIDDLE EAST AND NORTH AFRICA FINANCIAL ACTION TASK FORCE (MENAFATF)

Orgán na spôsob FATF zriadený pre regióny Blízkeho východu a severnej Afriky v roku 2004. MENAFATF je dobrovoľný a kooperatívny orgán, ktorý je nezávislý od akéhokoľvek iného medzinárodného orgánu alebo organizácie; vznikol na základe dohody medzi vládami svojich členov a nie je založený na medzinárodnej zmluve. Svoju prácu, predpisy, pravidlá a postupy si stanovuje sama a pri dosahovaní svojich cieľov spolupracuje s inými medzinárodnými orgánmi, najmä s FATF.

MILTECH (MILITARY TECHNOLOGY)

Nie je to zatiaľ štandardizovaný termín v rámci FATF odporúčaní ani smerníc AMLD. V praxi finančnej compliance a exportnej kontroly sa však vyskytuje v dvoch významoch:

i. Military Technology (vojenská/obranná technológia) – v kontexte exportnej kontroly a sankcií: tovar, softvér a technológie navrhnuté alebo upravené pre obranné účely, ktoré podliehajú prísnym režimom exportnej kontroly. Patria sem položky zahrnuté do Spoločného obranného materiálu EÚ (EÚ Common Military List), Wassenaarovho zoznamu, amerického ITAH (International Traffic in Arms Regulation) alebo EAR (export Administration Regulations). Z pohľadu AML/CFT predstavujú transakcie súvisiace s MilTech zvýšené riziko obchádzania sankcií a financovania proliferácie.

ii. (Dual_Use /MilTech Screening – kontrola protistrán a transakcií voči zoznamom entít zapojených do nelegálneho obchodu s obranným materiálom alebo technológiami s dvojakým použitím (dual-use).

MIRROR TRADE

Typ obchodu, ktorý zahŕňa nákup cenných papierov v jednej mene a následný predaj rovnakých cenných papierov v inej mene, pričom obe transakcie sú zvyčajne vykonané tým istým alebo spriazneným subjektom.

V kontexte AML/CFT sa zrkadlové obchody preslávili ako nástroj rozsiahleho prania špinavých peňazí najmä prípadom Deutsche Bank, kde boli

v rokoch 2011 až 2015 použité na presun približne 10 miliárd USD z Ruska do západných jurisdikcií – klienti nakupovali ruské akcie v rubľoch a prostredníctvom spriazneného subjektu ich súčasne predávali v londýnskom pobočke za doláre, čím efektívne konvertovali ruble pochybného pôvodu na doláre mimo dosahu ruských regulátorov. Zrkadlové obchody sú pritom zákerné práve preto, že každá individuálna transakcia môže vyzerať ako legitímna obchodná operácia – podozrivý je až vzorec koordinovaných nákupov a predajov medzi spriaznením osobami v rôznych jurisdikciách bez zjavného ekonomického opodstatnenia. Pre finančné inštitúcie vyplýva z tejto typológie povinnosť monitorovať nielen jednotlivé transakcie, ale aj vzorce obchodných aktivít naprieč účtami a jurisdikciami, osobitne sledovať koordinované transakcie medzi spriaznením osobami a vyhodnocovať ekonomickú racionalitu obchodných stratégií klientov – absencia legitímneho ekonomického dôvodu pre koordinované nákupy a predaje je kľúčovým varovným signálom zrkadlového obchodu.

MIXING/TUMBLING

Technika anonymizácie kryptomien, pri ktorej sa kryptomeny rôznych používateľov miešajú s cieľom zastrieť pôvod prostriedkov a sťažiť ich sledovanie. Mixéry (tumblers) sa používajú na prerušenie blockchain sledovateľnosti. FATF a orgány finančnej inteligencie klasifikujú používanie mixérov ako červenú vlajku pre potencionálne pranie špinavých peňazí.

MONETARY INSTRUMENTS

Kategória finančných nástrojov. Cestovné šeky, obchodovateľné nástroje vrátane osobných a obchodných šekov, oficiálne bankové šeky, pokladničné šeky, zmenky, peňažné poukážky, cenné papiere alebo akcie na doručiteľa. Peňažné nástroje sú spolu s menami zvyčajne zahrnuté do predpisov proti praniu špinavých peňazí vo väčšine krajín a finančné inštitúcie musia podávať správy a viesť záznamy o aktivitách klientov, ktoré sa ich týkajú.

V kontexte AML/CFT predstavujú peňažné nástroje rizikovú kategóriu z dôvodu ich prenosnosti, relatívnej anonymity a schopnosti uchovávať a prenášať hodnotu mimo bankového systému – vlastnosti, ktoré ich robia atraktívnymi pre pašovanie hodnôt cez hranice, štruktúrovanie platieb pod hranicou povinného hlásenia a konverziu hotovosti na zdanlivo legitímnejšiu formu aktíva. Osobitne rizikové sú nástroje na doručiteľa, ktoré nevyžadujú identifikáciu vlastníka a ich vlastníctvo sa prevádza samotným odovzdaním – práve preto väčšina jurisdikcií buď zakázala vydávanie nových nástrojov na doručiteľa alebo výrazne obmedzila ich používanie. Cezhraničná preprava peňažných nástrojov podlieha v mnohých jurisdikciách povinnosti deklarácie colným orgánom analogicky ako fyzická preprava hotovosti, pričom nedodržanie tejto povinnosti môže viesť ku konfiškácii nástroja a ďalším sankciám. Pre finančné inštitúcie vyplýva z práce s peňažnými nástrojmi povinnosť vedenia záznamov o ich vydávaní a preplatení, identifikácie klientov pri transakciách nad stanovené limity a monitorovania vzorcov naznačujúcich štruktúrovanie alebo iné zneužívanie týchto nástrojov na účely prania špinavých peňazí.

MONEY LAUNDERING

Proces utajovania alebo zakrývania existencie, zdroja, pohybu, miesta určenia alebo nezákonného použitia nezákonne nadobudnutého majetku alebo finančných prostriedkov s cieľom dosiahnuť, aby vyzerali ako legálne. Zvyčajne zahŕňa trojdielny systém: umiestnenie finančných prostriedkov do finančného systému, vrstvenie transakcií s cieľom zakryť zdroj, vlastníctvo a umiestnenie finančných prostriedkov a začlenenie finančných prostriedkov do spoločnosti vo forme držby, ktorá sa javí ako legálna. Definícia prania špinavých peňazí sa v jednotlivých krajinách, v ktorých sa uznáva za trestný čin, líši.

MONEY LAUNDERING REPORTING OFFICER (MLRO)

Termín používaný v rôznych medzinárodných pravidlách na označenie osoby zodpovednej za dohľad nad aktivitami a programom firmy proti praniu špinavých peňazí a za podávanie správ o podozrivých transakciách národnej FSJ (FIU). MLRO je kľúčovou osobou pri implementácii stratégií a politík proti praniu špinavých peňazí.

MONEY ORDER (PEŇAŽNÁ POUKÁŽKA)

Peňažný nástroj, ktorý sa zvyčajne kupuje za hotovosť v malých nominálnych hodnotách. Bežne ho používajú ľudia bez bežných účtov na platenie účtov alebo na platenie faktúr alebo nákupov, pri ktorých predajca neakceptuje osobný šek. Na rozdiel od osobného šeku je peňažná poukážka vystavená na vydávajúcu inštitúciu, nie na individuálny bankový účet, čo ju robí všeobecne akceptovateľným a dôveryhodným platobným prostriedkom.

V kontexte AML/CFT predstavuje peňažná poukážka klasický nástroj fázy umiestnenia v procese prania špinavých peňazí – nákupom série peňažných poukážok za hotovosť v hodnotách pod hranicou povinného hlásenia páchateľ konvertuje nelegálnu hotovosť na zdanlivo legitímny bankový nástroj, ktorý je ľahko prenosný, ťažko sledovateľný a prijímaný prakticky kdekoľvek. Typickým varovným signálom je nákup viacerých peňažných poukážok v rovnaký deň alebo v krátkom časovom období v hodnotách tesne pod reportingovou hranicou, nákup rôznymi osobami koordinovane v tej istej inštitúcii, poukážky vystavené na tretie osoby bez zjavného obchodného dôvodu a ich následné zaslanie do zahraničia. Vydavatelia peňažných poukážok – vrátane bánk, pošty a poskytovateľov peňažných služieb (MSB) – sú povinní identifikovať kupujúcich pri transakciách nad stanovené limity, monitorovať vzorce naznačujúce štruktúrovanie a podávať správy o podozrivých aktivitách príslušným orgánom.

MONEY SERVICES BUSINESS (MSB)

Osoba (fyzická alebo právnická), ktorá vykonáva niektorú z nasledujúcich činností, ak prekročí platnú regulačnú prahovú hodnotu, pričom sa vo všeobecnosti považuje za finančnú inštitúciu, na ktorú sa vzťahujú povinnosti v oblasti AML: obchodovanie s devízami, preplácanie šekov, vydávanie alebo predaj cestovných šekov alebo peňažných poukážok, poskytovanie alebo predaj predplateného prístupu, prevod peňazí.

MONEY TRANSFER SERVICE OR VALUE TRANSFER SERVICE

Finančná služba, ktorá prijíma hotovosť, šeky a iné peňažné nástroje, ktoré môžu uchovávať hodnotu na jednom mieste a vyplácať zodpovedajúcu sumu v hotovosti alebo inej forme príjemcovi na inom mieste prostredníctvom komunikácie, správy, prevodu alebo prostredníctvom zúčtovacej siete, do ktorej služba prevodu peňazí/hodnoty patrí. Transakcie vykonávané takýmito službami môžu zahŕňať jedného alebo viacerých sprostredkovateľov a konečnú platbu tretej strany. Službu prevodu peňazí alebo hodnoty môžu poskytovať osoby (fyzické alebo právnické) formálne prostredníctvom regulovaného finančného systému (napríklad bankové účty), neformálne prostredníctvom nebankových finančných inštitúcií a podnikateľských subjektov alebo mimo regulovaného systému. V niektorých jurisdikciách sa neformálne systémy označujú ako alternatívne služby prevodov alebo podzemné (či paralelné) bankové systémy. Podľa odporúčaní FATF: Služby prevodu peňazí alebo hodnôt (MVTS) sa vzťahujú na finančné služby, ktoré zahŕňajú prijímanie hotovosti, šekov, iných peňažných nástrojov alebo iných uchovávateľov hodnôt a platbu zodpovedajúcej sumy v hotovosti alebo inej forme príjemcovi prostredníctvom komunikácie, správy, prevodu alebo prostredníctvom zúčtovacej siete, do ktorej patrí poskytovateľ MVTS. Transakcie vykonávané takýmito službami môžu zahŕňať jedného alebo viacerých sprostredkovateľov a konečnú platbu tretej strane a môžu zahŕňať akékoľvek nové platobné metódy. Niekedy majú tieto služby väzby na konkrétne geografické regióny a označujú sa rôznymi špecifickými termínmi vrátane hawala, hundi a fej-čchen.

MONEYVAL

Výbor expertov pre hodnotenie opatrení proti praniu špinavých peňazí a financovaniu terorizmu - MONEYVAL je stálym monitorovacím orgánom

Rady Európy povereným úlohou posudzovať dodržiavanie hlavných medzinárodných noriem na boj proti praniu špinavých peňazí a financovaniu terorizmu a účinnosť ich uplatňovania, ako aj úlohou vydávať odporúčania vnútroštátnym orgánom v súvislosti s potrebnými zlepšeniami ich systémov. Prostredníctvom dynamického procesu vzájomných hodnotení, partnerského preskúmania a pravidelného sledovania svojich správ sa MONEYVAL usiluje zlepšiť kapacity vnútroštátnych orgánov na účinnejší boj proti praniu špinavých peňazí a financovaniu terorizmu. MONEYVAL (predtým PC-R-EV) bol zriadený v roku 1997 a jeho fungovanie upravujú všeobecné ustanovenia rezolúcie (2005) 47 o výboroch a podriadených orgánoch, ich mandáte a pracovných metódach. Výbor ministrov na svojom zasadnutí 13. októbra 2010 prijal rezolúciu CM/Res(2010)12 o štatúte Výboru expertov pre hodnotenie opatrení proti praniu špinavých peňazí a financovaniu terorizmu (MONEYVAL). Týmto štatútom sa MONEYVAL od 1. januára 2011 povyšuje na nezávislý monitorovací mechanizmus v rámci Rady Európy, ktorý sa zodpovedá priamo Výboru ministrov. Štatút MONEYVAL bol ďalej zmenený a doplnený v roku 2013 uznesením CM/Res(2013)13.

MONITORING

Prvok programu inštitúcie proti praniu špinavých peňazí, v rámci ktorého sa preveruje aktivita klienta z hľadiska neobvyklých alebo podozrivých vzorcov, trendov alebo odľahlých transakcií, ktoré nezodpovedajú bežnému vzorcu. Transakcie sa často monitorujú pomocou softvéru, ktorý zvažuje aktivitu vzhľadom na práh, ktorý sa považuje za „normálny a očakávaný“ pre daného klienta.

MULTILATERAL SANCTIONS

Mnohostranné sankcie sú obmedzenia, ktoré podporuje viac ako jedna krajina alebo subjekt. Môžu ich uložiť spojenci proti spoločnému nepriateľovi alebo na účely dosiahnutia väčšieho hospodárskeho a represívneho účinku.

MUTUAL EVALUATIONS

Proces vzájomného hodnotenia národných systémov AML/CFT z hľadiska súladu so štandardmi FATF na základe metodiky FATF. Hodnotenia sú vzájomné v tom zmysle, že zástupcovia všetkých členských štátov regionálnych orgánov typu FATF postupne hodnotia ostatné členské štáty v súlade s harmonogramom hodnotenia.

MUTUAL EVALUATION REPORT (MER)

Správy poskytujúce podrobný opis a analýzu systémov krajiny na obmedzenie finančnej trestnej činnosti na základe odporúčaní FATF. Hoci tieto správy nepredstavujú sankcie, majú potenciál ovplyvniť riziko, ktoré finančná inštitúcia podstúpi pri obchodovaní s konkrétnou krajinou alebo regiónom.

MUTUAL LEGAL ASSISTANCE TREATY (MLAT)

Zmluva o vzájomnej právnej pomoci (MLAT) je dohoda medzi dvoma alebo viacerými krajinami na účely zhromažďovania a výmeny informácií s cieľom presadzovať verejné alebo trestné právo. Žiadosť o vzájomnú právnu pomoc sa bežne používa na formálny výsluch podozrivého v trestnom konaní, ak má podozrivý pobyt v cudzej krajine.

NAME SCREENING

Proces porovnávania interného záznamu (t. j. klienta, protistrany, spriaznenej strany účtu) so záznamom na sankčnom zozname, a to buď manuálne, alebo prostredníctvom automatického nástroja na kontrolu. Skríning mien môže zahŕňať aj dávkový skríning mien, ktorý umožňuje firme pravidelne preverovať celú svoju klientsku základňu pomocou automatických skríningových nástrojov. Pri prijímaní nových zákazníkov sa pred prijatím nového vzťahu so zákazníkom vykonáva kontrola mena na základe sankčných zoznamov, a to v reálnom čase. Skríning mien tvorí súčasť vstupných kontrol, ktoré finančnej inštitúcii poskytujú viac príležitostí na zhromažďovanie informácií o SDD.

NAMING CONVENTIONS

Spôsoby (všeobecne dohodnutá alebo známa schéma na pomenovanie), akými sa meno jednotlivca dáva alebo používa. Mená sa môžu prezentovať mnohými spôsobmi, ktoré do veľkej miery závisia od krajiny alebo kultúrnych noriem krajiny, v ktorej sa jednotlivec narodil alebo vyrastal.

NATIONAL RISK ASSESSMENT (NRA) – NÁRODNÉ HODNOTENIE RIZÍK

Systematický proces, ktorým krajina identifikuje, hodnotí a chápe riziká prania špinavých peňazí a financovania terorizmu, ktorým je vybavená. NRA je základným predpokladom prístupu založeného na riziku podľa odporúčaní FATF a slúži ako základ pre prioritizáciu zdrojov a opatrení v oblasti AML/CFT. Výsledky NRA ovplyvňujú regulačné požiadavky na finančné a nefinančné inštitúcie.

NESTED ACCOUNT

Využívanie korešpondenčného vzťahu banky viacerými podkladovými bankami alebo finančnými inštitúciami prostredníctvom ich vzťahov s priamym klientom korešpondenčnej banky. Základné respondentské banky alebo finančné inštitúcie vykonávajú transakcie a získavajú prístup k iným finančným službám bez toho, aby boli priamymi klientmi korešpondenčnej banky.

V kontexte AML/CFT predstavuje vnorený účet závažné riziko, keďže efektívne skrýva skutočnú totožnosť a povahu subjektov využívajúcich finančný systém za fasádou priameho klienta korešpondenčnej banky – korešpondenčná banka vykonáva due diligence voči svojmu priamemu klientovi, avšak nemá žiadnu priamu viditeľnosť ani kontrolu nad skutočnými koncovými užívateľmi, ktorí prostredníctvom neho vykonávajú transakcie. Toto uspôsobenie je osobitne rizikové, keď priamy klient korešpondenčnej banky pôsobí v jurisdikcii s nízkymi AML/CFT štandardmi a umožňuje prístup k svojmu účtu inštitúciám alebo subjektom, ktoré by priamy prístup ku korešpondenčnej banke nikdy nezískali – napríklad pre nedostatočné AML/CFT kontroly, sankčné prepojenia alebo iné rizikové faktory. Odporúčania FATF a usmernenia pre korešpondenčné bankovníctvo preto vyžadujú, aby korešpondenčné banky pri nadväzovaní vzťahov s respondentskými bankami aktívne zisťovali, či respondent umožňuje vnorený prístup tretím subjektom, a ak áno, požadovali dostatočné informácie o týchto subjektoch a zavedených kontrolách; tolerovanie vnorených účtov bez primeranej transparentnosti a kontroly je pre regulátorov závažným varovným signálom nedostatočného riadenia rizík korešpondenčného bankovníctva.

NESTING

Postup, keď respondentská banka poskytuje nadväzujúce korešpondenčné služby iným finančným inštitúciám a tieto transakcie spracúva prostredníctvom svojho vlastného korešpondenčného účtu. Korešpondenčná banka tak spracúva transakcie pre finančné inštitúcie, u ktorých nevykonala hĺbkovú kontrolu. Hoci ide o bežnú súčasť korešpondenčného bankovníctva, vyžaduje si, aby korešpondenčná banka vykonala zvýšenú hĺbkovú kontrolu programu AML respondenta s cieľom primerane znížiť riziko spracovania transakcií klientov klienta.

V kontexte AML/CFT predstavuje nesting zásadnú výzvu pre riadenie rizík korešpondenčného bankovníctva – korešpondenčná banka je vystavená rizikám, ktoré nie sú priamo viditeľné a nekontrolovateľné, keďže nemá priamy vzťah ani due diligence voči inštitúciám skrytým za jej priamym

respondentom. Hoci nesting je bežnou a legitímnou súčasťou globálneho korešpondenčného bankovníctva umožňujúcou menším inštitúciám v rozvíjajúcich sa jurisdikciách prístup k medzinárodnému finančnému systému, jeho rizikovosť priamo závisí od kvality AML/CFT programu respondentskej banky a jej vlastných kontrol voči inštitúciám, ktorým poskytuje vnorené služby. Odporúčania FATF a usmernenia pre korešpondenčné bankovníctvo preto vyžadujú od korešpondenčných bánk aktívne zisťovanie rozsahu nestingových aktivít respondenta, dôkladné hodnotenie kvality AML/CFT programu respondenta vrátane jeho schopnosti riadiť riziká spojené s vnoreným prístupom, získanie dostatočných informácií o inštitúciách využívajúcich vnorený prístup a zavedenie primeraných kontrol zodpovedajúcich riziku vyplývajúcemu z celého reťazca korešpondenčných vzťahov; korešpondenčné banky, ktoré tolerujú nesting bez primeranej transparentnosti a due diligence, preberajú zodpovednosť za transakcie subjektov, ktoré nikdy nepreverili, čo môže viesť k závažným regulačným sankciám v prípade zneužitia tohto reťazca na pranie špinavých peňazí alebo obchádzanie sankcií.

NTF (NON-FUNGIBLE TOKEN)

Jedinečné digitálne aktívum zaznamenané na blockchaine, ktoré reprezentuje vlastníctvo konkrétneho digitálneho alebo fyzického predmetu (umelecké diela, herné predmety, nehnuteľnosti). Z pohľadu AML/CFT sú NFT predmetom rastúceho záujmu regulátorov, keďže môžu byť použité na pranie špinavých peňazí prostredníctvom manipulácie s cenami alebo wash tradingu. FATF zahrnul NFT do svojich usmernení o virtuálnych (krypto) aktívach.

NOMINEE DIRECTOR OR SHAREHOLDER

Osoba, ktorá nie je skutočným riaditeľom alebo akcionárom spoločnosti, ale je poverená konať v mene jej riaditeľov alebo akcionárov. Hoci používanie nominovaných akcionárov tiež rýchlo klesá, používanie nominovaných riaditeľov je stále bežné.

V kontexte AML/CFT predstavujú nominálni riaditelia a akcionári jeden z najrozšírenejších nástrojov zakrývania skutočného vlastníctva a kontroly nad právnickými osobami – ich využívanie je priamym útokom na princíp transparentnosti skutočného vlastníctva, ktorý je základom celého AML/CFT systému. Hoci používanie nominálnych akcionárov postupne klesá v dôsledku zavedenia registrov skutočných vlastníkov a sprísnenia regulačných požiadaviek, nominálni riaditelia zostávajú bežnou praxou najmä v offshore jurisdikciách a pri medzinárodných podnikových štruktúrach. FATF odporúčanie č. 24 explicitne vyžaduje, aby krajiny zabezpečili transparentnosť pri využívaní nominálnych osôb – poskytovatelia nominálnych služieb musia uchovávať informácie o skutočných principáloch a sprístupňovať ich príslušným orgánom, pričom samotná skutočnosť, že osoba vystupuje ako nominálny riaditeľ alebo akcionár, musí byť zaznamenaná a identifikovateľná. Pre finančné inštitúcie je identifikácia nominálnych osôb v štruktúrach klientov kritickou súčasťou KYB procesu – nestačí identifikovať formálnych riaditeľov a akcionárov zapísaných v obchodnom registri, ale je nevyhnutné aktívne preskúmať, či títo jednotlivci skutočne vykonávajú riadiacu funkciu alebo slúžia len ako nominálne osoby zakrývajúce skutočného vlastníka; indikátormi nominálneho vzťahu sú napríklad rovnaká osoba vystupujúca ako riaditeľ vo veľkom počte nesúvisiacich spoločností, absencia skutočných znalostí o podniku pri rozhovore s klientom alebo existencia splnomocnení prenášajúcich skutočné rozhodovacie právomoci na inú osobu.

NON-CONVICTION BASED CONFISCATION

Konfiškácia bez odsúdenia znamená konfiškáciu prostredníctvom súdneho konania v súvislosti s trestným činom, pre ktorý sa nevyžaduje odsúdenie.

NON-COOPERATIVE COUNTRIES & TERRITORIES (NCCT)

Krajiny, ktoré FATF považuje za nespolupracujúce v celosvetovom boji proti praniu špinavých peňazí a financovaniu terorizmu. Hlavným cieľom iniciatívy nespolupracujúcich krajín a území (NCCT) bolo znížiť zraniteľnosť finančného systému voči praniu špinavých peňazí tým, že sa zabezpečí, aby všetky finančné centrá prijali a vykonávali opatrenia na prevenciu, odhaľovanie a trestanie prania špinavých peňazí v súlade s medzinárodne uznávanými normami.

NON-GOVERNMENTAL ORGANIZATION (NGO)

Neziskové organizácie, ktoré nie sú priamo prepojené s vládami konkrétnych krajín a vykonávajú rôzne služby a humanitárne funkcie vrátane predkladania problémov občanov vládam, obhajoby cieľov a podpory politickej účasti. Predpisy niektorých krajín proti praniu špinavých peňazí pre mimovládne organizácie majú stále medzery, ktoré by podľa niektorých obáv mohli využiť teroristi alebo sympatizanti teroristov, ktorí sa snažia tajne presúvať peniaze.

NON-PROFIT ORGANIZATIONS (NPO)

V závislosti od jurisdikcie a právneho systému môžu mať rôzne formy, vrátane združení, nadácií, výborov na získavanie finančných prostriedkov, verejnoprospešných organizácií, spoločností vo verejnom záujme, spoločností s ručením obmedzeným a verejnoprospešných inštitúcií. FATF navrhla postupy, ktoré majú orgánom pomôcť chrániť organizácie, ktoré zhromažďujú alebo vyplácajú finančné prostriedky na charitatívne, náboženské, kultúrne, vzdelávacie, sociálne alebo bratské účely, pred zneužitím alebo zneužitím zo strany financovateľov terorizmu. V júni 2016 a znova k októbri 2023 FATF revidoval Odporúčanie č. 8. Nový prístup je výrazne cielenejší – krajiny nemajú pristupovať k celému sektoru NPO ako k vysokorizikovému, ale majú identifikovať iba tie organizácie, ktoré sú skutočne vystavené riziku zneužitia na financovanie terorizmu.

NON-PROLIFERATION TREATY (NPT)

Zmluva OSN o nešírení jadrových zbraní bola podpísaná v roku 1968 a vstúpila do platnosti v marci 1970. Zmluva o nešírení jadrových zbraní upevnila záväzok signatárskych krajín zabrániť šíreniu jadrových zbraní. Jej cieľom bolo minimalizovať riziko použitia jadrových zbraní v konflikte, ktorý by mohol mať za následok značné škody. Rovnako sa NPT snažila zabrániť tomu, aby sa tieto zbrane dostali do rúk nečestných krajín a teroristov.

OFFICE FOR FOREIGN ASSETS CONTROL (OFAC)

Úrad pre kontrolu zahraničných aktív (OFAC) amerického ministerstva financií spravuje a presadzuje hospodárske a obchodné sankcie na základe cieľov zahraničnej politiky a národnej bezpečnosti USA voči vybraným zahraničným krajinám a režimom, teroristom, medzinárodným obchodníkom s narkotikami, osobám zapojeným do činností súvisiacich so šírením zbraní hromadného ničenia a iným hrozbám pre národnú bezpečnosť, zahraničnú politiku alebo hospodárstvo USA. Je súčasťou zahraničnej politiky USA a medzinárodných organizácií, ako je OSN, voči vybraným zahraničným krajinám. Často spolupracuje s ďalšími agentúrami, ako je ministerstvo zahraničných vecí, s cieľom dohliadať na ciele národnej bezpečnosti. Hlavnou súčasťou povinností agentúry je vytváranie a vedenie zoznamu osobitne označených osôb (SDN).

OFFICE OF THE SUPERINTENDENT OF FINANCIAL INTITUTIONS (OSFI)

Hlavná agentúra regulujúca finančné inštitúcie v Kanade. OSFI bol zriadený 2. júla 1987 zákonom o Úrade superintendenta finančných inštitúcií (ďalej len „zákon o OSFI“). Týmto právnym predpisom sa vytvoril jediný regulačný orgán zodpovedný za reguláciu a dohľad nad všetkými federálne schválenými, licencovanými alebo registrovanými bankami, poisťovňami, správcovskými a úverovými spoločnosťami, bratskými benefitnými spoločnosťami a súkromnými penzijnými plánmi.

OFFSHORE

Doslova mimo svojej domovskej krajiny - ak žijete v Európe, USA sú „offshore“. V lexikóne prania špinavých peňazí sa tento pojem vzťahuje na jurisdikcie považované za priaznivé pre zahraničné investície z dôvodu nízkeho alebo žiadneho zdanenia alebo prísnych predpisov týkajúcich sa bankového tajomstva. Vo všeobecnom ponímaní sa využíva aj pojem „offshore spoločnosť“ alebo „offshore korporácia. Offshore spoločnosť môže byť odkazom na: (i) spoločnosť, skupinu alebo niekedy jej divíziu, ktorá sa zaoberá offshoringom obchodných procesov alebo sú to medzinárodné obchodné spoločnosti (IBC) alebo iné typy právnických osôb, ktoré sú založené podľa zákonov jurisdikcie, ktorá zakazuje alebo obmedzuje miestne hospodárske činnosti. Prvé použitie (spoločnosti založené v offshore jurisdikciách) je pravdepodobne bežnejším použitím tohto pojmu. V ojedinelých prípadoch sa tento termín môže používať aj v súvislosti so spoločnosťami s offshore aktivitami v oblasti ropy a zemného plynu.

OFFSHORE BANKING LICENSE

Offshore banková licencia umožňuje držiteľovi prevádzkovať banku v jednej krajine, ktorá poskytuje služby vkladateľom s trvalým pobytom v iných krajinách. Licenciu vydáva krajina, v ktorej sa banka prevádzkuje, čo nemusí byť nevyhnutne krajina, ktorej je držiteľ občanom alebo rezidentom. Tieto krajiny majú zvyčajne nízke alebo dokonca nulové daňové sadzby, čo znamená, že vkladatelia môžu znížiť svoje daňové náklady tým, že budú bankovať v tejto krajine, a nie vo svojej krajine. Mnohé krajiny vrátane Spojených štátov však stále požadujú, aby rezidenti platili daň zo svojich offshore bankových účtov, ak sú daňoví úradníci schopní preukázať existenciu takýchto účtov.

OFFSHORE FINANCE

Offshore financovanie je najjednoduchšie povedané poskytovanie finančných služieb bankami a inými sprostredkovateľmi nerezidentom. Tieto služby zahŕňajú požičiavanie peňazí od nerezidentov a poskytovanie úverov nerezidentom. Môže mať podobu pôžičiek podnikom a iným finančným inštitúciám, ktoré sú financované záväzkami voči pobočkám banky poskytujúcej pôžičku inde alebo účastníkom trhu. Môže mať aj podobu prijímania vkladov od fyzických osôb a investovania výnosov na finančných trhoch inde. Niektoré z týchto činností sú zachytené v štatistikách, ktoré zverejňuje Banka pre medzinárodné zúčtovanie (BIS). Pravdepodobne oveľa významnejšie sú prostriedky, ktoré finančné inštitúcie spravujú na riziko klienta. Takáto podsúvahová alebo fiduciárna činnosť sa v dostupných štatistikách spravidla neuvádza. Okrem toho sa predpokladá, že významné finančné prostriedky držia v OFS podielové fondy a trusty, tzv. medzinárodné obchodné spoločnosti (International Business Companies - IBC) alebo iní sprostredkovatelia, ktorí nie sú spojení s finančnými inštitúciami.

OFFSHORE FINANCIAL CENTER (OFC)

V najširšom zmysle možno OFC definovať ako akékoľvek finančné centrum, v ktorom sa vykonávajú offshore aktivity. Táto definícia by zahŕňala všetky hlavné finančné centrá na svete. V takýchto centrách môže byť malý rozdiel medzi on- a offshore obchodmi, t. j. pôžička nerezidentovi môže byť financovaná na vlastnom trhu centra, kde dodávatelia finančných prostriedkov môžu byť rezidenti alebo nerezidenti. Podobne aj správca fondu nemusí rozlišovať medzi finančnými prostriedkami klientov rezidentov a nerezidentov. Praktickejšia definícia OFC je centrum, v ktorom je väčšina aktivít finančného sektora na oboch stranách súvahy offshore (t. j. protistrany väčšiny záväzkov a aktív finančných inštitúcií sú nerezidenti), kde sa transakcie iniciujú inde a kde väčšinu zúčastnených inštitúcií kontrolujú nerezidenti. Preto sa OFC zvyčajne označujú ako (i) jurisdikcie, ktoré majú relatívne veľký počet finančných inštitúcií zapojených predovšetkým do obchodov s nerezidentmi, (ii) finančné systémy, ktorých zahraničné aktíva a pasíva sú v nepomere k domácemu finančnému sprostredkovaniu určenému na financovanie domácej ekonomiky, a (iii) populárnejšie centrá, ktoré poskytujú niektoré alebo všetky z týchto služieb: nízke alebo nulové zdanenie; mierna alebo ľahká finančná regulácia; bankové tajomstvo a anonymita. OFC sa v minulosti nachádzali v Karibiku alebo na stredomorských ostrovoch, aby boli v primeranej blízkosti hlavných finančných centier v USA a Európe.

OFFSHORE GROUP OF BANKING SUPERVISORS (OGBS), GROUP OF INTERNATIONAL FINANCE CENTRE SUPERVISORS

Po prvej medzinárodnej konferencii orgánov bankového dohľadu, ktorá sa konala v roku 1979 v Londýne, Bazilejský výbor pre bankový dohľad (BCBS) rozhodol, že by bolo vhodné iniciovať stretnutie orgánov bankového dohľadu zastupujúcich menšie zámorské jurisdikcie, ako sme my. Koncom 70. rokov minulého storočia došlo k výraznému rozšíreniu medzinárodných úverových aktivít, pričom mnohé úvery boli z daňových dôvodov zaúčtované v zahraničí. Členské krajiny Bazilejského výboru sa obávali, že banky, za ktoré boli zodpovedné, boli ohrozené, pretože sa obávali, že ich dcérske spoločnosti alebo pobočky v takýchto centrách nepodliehajú dostatočnému dohľadu. Na podnet BCBS bola následne vytvorená Offshore skupina orgánov bankového dohľadu ako združenie príslušných orgánov zaoberajúcich sa dohľadom nad bankami a súvisiacimi finančnými službami, ktoré sa primárne zaoberajú cezhraničnými aktivitami. Prvé stretnutie skupiny sa uskutočnilo v Bazileji, kde sa zástupcovia viacerých relevantných jurisdikcií stretli s členmi Bazilejského výboru. Návrh na vytvorenie skupiny privítali všetci zainteresovaní. Pri zachovaní úzkych pracovných vzťahov s BCBS sa skupina odvtedy vyvinula v orgán zastupujúci záujmy členských jurisdikcií v oblasti bankového dohľadu, postupov AML/CFT, dohľadu nad fondmi a činnosťami s cennými papiermi a regulácie poskytovateľov dôveryhodných a obchodných služieb (TCSP). V polovici 90. rokov sa skupina stala pozorovateľským orgánom FATF. Je členom regionálnej poradnej skupiny FSB pre Európu a členom Bazilejskej poradnej skupiny. Na základe významných skúseností členov GIFCS s udeľovaním licencií a reguláciou TCSP bol v októbri 2014 vydaný nový štandard pre reguláciu TCSP. Tento štandard sa teraz rozvinul do úplného režimu zahŕňajúceho multilaterálne memorandum o porozumení, vzájomné hodnotenia dodržiavania štandardu zo strany členov a stretnutia kolégií orgánov dohľadu s cieľom koordinovať prístupy dohľadu k skupinám TCSP. V marci 2011 sa skupina rozhodla lepšie vyjadriť rozsah svojich činností zmenou názvu na Skupinu orgánov dohľadu medzinárodných finančných centier. V súčasnosti sa skupina zúčastňuje najmä na iniciatívach s BCBS, FATF, Radou pre finančnú stabilitu a IOSCO. Väčšina členov GIFCS je plnoprávnymi signatármi MMOU IOSCO a viacerí sa priamo zúčastňujú na činnosti pracovných skupín IOSCO.

ONGOING DUE DILIGENCE

Priebežné monitorovanie obchodného vzťahu vrátane kontroly transakcií s cieľom zabezpečiť, že transakcie sú konzistentné s vedomosťami inštitúcie o zákazníkovi, jeho obchodnom a rizikovom profile. Zahŕňa pravidelnú aktualizáciu informácií o zákazníkovi a opätovnú previerku pri výskyte spúšťacích udalostí. Je kľúčovou povinnosťou v rámci CDD podľa smerníc AMLD a odporúčaní FATF.

OPERATIONAL RISK

Riziko priamej alebo nepriamej straty operácií v dôsledku nevhodných alebo zlyhaných interných procesov, ľudí alebo systémov alebo v dôsledku vonkajších udalostí. Vnímanie verejnosti, že banka nie je schopná efektívne riadiť svoje operačné riziko, môže narušiť alebo poškodiť podnikanie banky.

V kontexte AML/CFT má operačné riziko osobitnú dimenziu – zlyhania v AML/CFT procesoch, systémoch alebo ľudskom faktore priamo generujú operačné riziko s potenciálne devastujúcimi finančnými a reputačnými následkami. Typické zdroje operačného rizika v oblasti AML/CFT zahŕňajú zlyhania technických systémov transakčného monitoringu

alebo sankčného screeningu spôsobujúce neidentifikované porušenia, procesné zlyhania vyplývajúce z nedostatočne zdokumentovaných alebo neaktualizovaných postupov, ľudské zlyhania zahŕňajúce nedostatočne vyškolených zamestnancov, interné podvody alebo nedbanlivosť pri vyhodnocovaní alertov, zlyhania tretích strán ako sú poskytovatelia outsourcovaných compliance služieb alebo dodávatelia technologických riešení a vonkajšie udalosti ako kybernetické útoky narúšajúce integritu AML/CFT systémov. Prepojenie operačného rizika s AML/CFT je obojsmerné – AML/CFT zlyhania generujú operačné riziko vo forme regulačných pokút, nákladov na nápravu a reputačných škôd, zatiaľ čo operačné zlyhania v iných oblastiach môžu vytvárať zraniteľnosti zneužiteľné na pranie špinavých peňazí; regulátori preto očakávajú, že riadenie operačného rizika a AML/CFT rizika sú integrované do jednotného rámca riadenia rizík inštitúcie, nie spravované izolovane ako samostatné disciplíny.

ORDERING FINANCIAL INSTITUTION

Vzťahuje sa na finančnú inštitúciu, ktorá iniciuje bankový prevod a prevedie finančné prostriedky po prijatí žiadosti o bankový prevod v mene príkazcu (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 16).

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD)

Organizácia pre hospodársku spoluprácu a rozvoj (OECD) je jedinečným fórom, na ktorom vlády 37 demokratických krajín s trhovým hospodárstvom spolupracujú na tvorbe politických noriem na podporu udržateľného hospodárskeho rastu a v máji 2021 sa Kostarika stala ďalším členom, čím celkový počet stúpol na 38. OECD poskytuje prostredie, v ktorom si vlády môžu porovnávať skúsenosti, hľadať odpovede na spoločné výzvy, identifikovať osvedčené postupy a rozvíjať vysoké štandardy hospodárskej politiky. OECD je už viac ako 50 rokov spoľahlivým zdrojom analýzy politík a hospodárskych údajov založených na dôkazoch. Spojené štáty spolupracujú s ostatnými členmi na posilnení transparentnosti, zodpovednosti, rozpočtovej disciplíny a schopnosti reagovať na priority členov OECD. Členské krajiny OECD dnes tvoria tri pätiny svetového HDP, tri štvrtiny svetového obchodu, viac ako 90 % globálnej oficiálnej rozvojovej pomoci, polovicu svetovej spotreby energie a 18 % svetovej populácie. Spolu so svojimi sesterskými agentúrami, Medzinárodnou energetickou agentúrou (IEA) a Agentúrou pre jadrovú energiu (NEA), OECD pomáha Spojeným štátom a ich partnerom využívať výhody a čeliť výzvam globálnej ekonomiky podporou zdravých hospodárskych politík, voľnejších trhov, efektívnejšieho využívania zdrojov a lepších inovácií prostredníctvom vedy a techniky.

ORIGINATOR

Majiteľ účtu alebo, ak účet neexistuje, osoba (fyzická alebo právnická), ktorá dáva príkaz finančnej inštitúcii na vykonanie bankového prevodu. Príkazca je iniciujúcou stranou platobného reťazca, od ktorej vychádza inštrukcia na presun finančných prostriedkov.

V kontexte AML/CFT je identifikácia a overenie príkazcu jednou z kľúčových povinností vyplývajúcich z odporúčania FATF č. 16 (Travel Rule) a nariadenia EÚ o transfere fondov (2023/1113) – každý bankový prevod musí byť sprevádzaný presnými a úplnými informáciami o príkazcovi vrátane mena, čísla účtu alebo jedinečného identifikátora transakcie a adresy, národného identifikačného čísla alebo dátumu a miesta narodenia. Povinnosť zabezpečiť úplnosť a presnosť informácií o príkazcovi leží primárne na finančnej inštitúcii príkazcu, ktorá je zároveň zodpovedná za to, že tieto informácie sprevádzajú platbu počas celého platobného reťazca až po prijímajúcu finančnú inštitúciu. Absencia, neúplnosť alebo nepresnosť informácií o príkazcovi je jedným z najvýznamnejších varovných signálov pri spracovaní medzinárodných platieb – môže naznačovať pokus o anonymizáciu platby, obchádzanie sankčného screeningu alebo stripping identifikačných údajov; prijímajúce a sprostredkujúce finančné inštitúcie sú povinné pri zistení chýbajúcich informácií o príkazcovi buď požiadať o ich doplnenie, obmedziť transakciu alebo ju odmietnuť a zvážiť podanie oznámenia o podozrivej aktivite.

PALERMO CONVENTION

Dohovor OSN proti nadnárodnému organizovanému zločinu, prijatý rezolúciou Valného zhromaždenia 55/25 z 15. novembra 2000, je hlavným medzinárodným nástrojom v boji proti nadnárodnému organizovanému zločinu. Bol otvorený na podpis členským štátom na politickej konferencii na vysokej úrovni, ktorá sa na tento účel konala 12. - 15. decembra 2000 v Palerme v Taliansku, a nadobudol platnosť 29. septembra 2003. Dohovor ďalej dopĺňajú tri protokoly, ktoré sa zameriavajú na konkrétne oblasti a prejavy organizovaného zločinu: Protokol o prevencii, potláčaní a trestaní obchodovania s ľuďmi, najmä so ženami a deťmi; Protokol proti pašovaniu migrantov po súši, mori a letecky; a Protokol proti nedovolenej výrobe a obchodovaniu so strelnými zbraňami, ich súčasťami a komponentmi a strelivom. Krajiny sa musia stať zmluvnými stranami samotného dohovoru skôr, ako sa môžu stať zmluvnými stranami ktorémukoľvek z protokolov. Dohovor predstavuje významný krok vpred v boji proti nadnárodnému organizovanému zločinu a znamená, že členské štáty uznávajú závažnosť problémov, ktoré predstavuje, ako aj potrebu podporovať a posilňovať úzku medzinárodnú spoluprácu s cieľom riešiť tieto problémy. Štáty, ktoré ratifikujú tento nástroj, sa zaväzujú prijať sériu opatrení proti nadnárodnému organizovanému zločinu vrátane vytvorenia vnútroštátnych trestných činov (účasť v organizovanej zločineckej skupine, pranie špinavých peňazí, korupcia a marenie spravodlivosti); prijatia nových a rozsiahlych rámcov pre vydávanie, vzájomnú právnu pomoc a spoluprácu v oblasti presadzovania práva; a podpory odbornej prípravy a technickej pomoci pri budovaní alebo zvyšovaní potrebných kapacít vnútroštátnych orgánov.

PARTIAL MATCH

Výsledok vygenerovaný pomocou AST. Čiastočná zhoda znamená, že kontrolovaný subjekt je dostatočne podobný sankcionovanému subjektu na základe fuzzy logiky a prípadne ďalších identifikačných faktorov, ako je dátum narodenia. Čiastočná zhoda si vyžaduje ďalší ľudský zásah, aby sa určilo, či je zhoda cieľová (alebo skutočná), t. j. či je meno, ktoré sa preveruje, rovnakým subjektom ako sankcionovaný cieľ.

PASS-THROUGH SANCTIONS RISK

Nesprávny predpoklad, že sankčné riziká spojené s pridruženými alebo dcérskymi spoločnosťami zákazníka sú jednoducho problémom, ktorý musí posúdiť a riadiť zákazník. Regulačné orgány v Spojenom kráľovstve a Spojených štátoch vyžadujú, aby všetky strany v rámci transakčného reťazca kontrolovali možné sankčné riziká. Je dôležité, aby finančné inštitúcie žiadali a preverovali informácie o pridružených a dcérskych spoločnostiach zákazníka.

PAYABLE THROUGH ACCOUNT

Transakčný účet otvorený v depozitnej inštitúcii zahraničnou finančnou inštitúciou, prostredníctvom ktorého sa klienti zahraničnej inštitúcie priamo alebo prostredníctvom podúčtov zúčastňujú na bankových činnostiach a transakciách takým spôsobom, že klienti finančnej inštitúcie majú priamu kontrolu nad prostriedkami na účte. Tieto účty predstavujú riziko pre depozitné inštitúcie, ktoré sú ich majiteľmi, pretože môže byť ťažké vykonať hĺbkovú kontrolu klientov zahraničných inštitúcií, ktorí v konečnom dôsledku používajú účty PTA.

PAYMENT SCREENING

Metóda kontroly, ktorá sa zameriava na kontrolu platobných správ. Na rozdiel od kontroly mien sa kontrola platieb vykonáva u súčasných zákazníkov

a vykonáva sa pred spracovaním platby alebo správy. Skríning platieb spočíva v tom, že platobné správy používajú preddefinované šablóny, kódy a skratky na opis určitých informácií. Informácie uvedené v týchto preddefinovaných šablónach zvyčajne poskytuje tretia strana, preto má firma len malú, ak vôbec nejakú, kontrolu nad tým, ako sú údaje prezentované.

PAYMENTS, CROSS BORDER

Platby, ktoré sa týkajú viac ako jednej krajiny, či už fyzickou prepravou hotovosti cez medzinárodnú hranicu, alebo elektronickým prevodom peňazí z jednej krajiny do druhej.

PHYSICAL CROSS-BORDER TRANSPORTATION

sa vzťahuje na akúkoľvek prichádzajúcu alebo odchádzajúcu fyzickú prepravu meny alebo HND z jednej krajiny do druhej. Tento pojem zahŕňa tieto spôsoby prepravy: 1) fyzickú prepravu fyzickou osobou alebo v sprievodnej batožine alebo vozidle tejto osoby; 2) prepravu peňazí alebo BNI prostredníctvom kontajnerového nákladu alebo 3) zasielanie peňazí alebo BNI poštou fyzickou alebo právnickou osobou (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 32).

PHYSICAL PRESENCE

Existencia skutočného kamenného sídla s významným manažmentom inštitúcie, ktorá sa fyzicky nachádza v danej krajine, kde vedie obchodné záznamy a podlieha dohľadu. Samotná existencia miestneho zástupcu alebo zamestnancov na nízkej úrovni nepredstavuje fyzickú prítomnosť.

PLACEMENT

Prvá a najrizikovejšia fáza procesu prania špinavých peňazí: fyzické nakladanie s príjmami pochádzajúcimi z nezákonnej/protiprávnej činnosti do legálneho finančného systému alebo ekonomiky.

V kontexte AML/CFT je fáza umiestnenia kritickým bodom celého procesu prania špinavých peňazí z dvoch dôvodov – je to moment, keď sú nelegálne prostriedky najzraniteľnejšie a najpriamejšie vystavené riziku odhalenia, keďže ich pôvod je ešte bezprostredne spojený s trestnou činnosťou, a zároveň je to fáza, v ktorej majú finančné inštitúcie najväčšiu príležitosť prerušiť celý proces ešte pred tým, než dôjde k jeho ďalšiemu zakrytiu. Typické techniky umiestnenia zahŕňajú hotovostné vklady na bankové účty, často štruktúrované pod hranicou povinného hlásenia (smurfing), využívanie zmenární a poskytovateľov peňažných služieb na konverziu hotovosti na iné nástroje, vkladanie hotovosti do cash-intensive businesses zmiešaním s legitímnymi tržbami (asset mingling), nákup peňažných poukážok, bankových šekov alebo iných prenosných peňažných nástrojov za hotovosť, pašovanie fyzickej hotovosti cez hranice do jurisdikcií s nižšími AML/CFT štandardmi, využívanie kasín na konverziu hotovosti na výhry (bill stuffing) a čoraz rozšírenejšiu konverziu hotovosti na virtuálne aktíva prostredníctvom kryptomenových búrz alebo Bitcoin bankomatov s nedostatočnými KYC požiadavkami. Práve zameranie kontrolných mechanizmov na fázu umiestnenia je základnou logikou povinnosti hlásiť hotovostné transakcie nad stanovené limity, požiadaviek na identifikáciu pri hotovostných transakciách a zákazu platby v hotovosti nad určitú sumu – každé z týchto opatrení smeruje k tomu, aby bolo zavedenie nelegálnych prostriedkov do finančného systému čo najťažšie a najsledovateľnejšie.

POLITICALLY EXPOSED PERSON (PEP)

Zahraničné PEP sú osoby, ktoré sú alebo boli poverené významnými verejnými funkciami v cudzej krajine, napríklad hlavy štátov alebo vlád, vysokí politici, vysokí vládni, súdni alebo vojenskí úradníci, vrcholoví manažéri štátnych spoločností, významní predstavitelia politických strán. Domáci PEP sú osoby, ktoré sú alebo boli v domácej krajine poverené významnými verejnými funkciami, napríklad hlavy štátov alebo vlád, vysokí politici, vysokí vládni, súdni alebo vojenskí úradníci, vedúci predstavitelia štátnych spoločností, významní predstavitelia politických strán. Osoby, ktoré sú alebo boli poverené významnou funkciou v medzinárodnej organizácii, sa vzťahujú na členov vyššieho manažmentu, t. j. riaditeľov, zástupcov riaditeľov a členov správnej rady alebo rovnocenných funkcií. Definícia PEP nemá zahŕňať stredne postavené alebo nižšie postavené osoby vo vyššie uvedených kategóriách.

PONZI SCHEME/PYRAMID SCHEME

Systém prania špinavých peňazí pomenovaný podľa Charlesa Ponziho, talianskeho prisťahovalca, ktorý strávil 10 rokov vo väzení v USA za podvod, v rámci ktorého pripravil 40 000 ľudí o 15 000 000 dolárov. Ponziho meno sa stalo synonymom použitia peňazí nových investorov na vyplatenie predchádzajúcich investorov. Ponziho schémy zahŕňajú falošné, neexistujúce investičné schémy, v ktorých sú investori podvedení, aby investovali na základe prísľubu nezvyčajne atraktívnych výnosov. Prevádzkovateľ schémy môže pokračovať v činnosti tým, že vypláca prvých investorov peniazmi od nových investorov, až kým sa schéma nezrúti pod vlastnou váhou a/alebo kým organizátor nezmizne so zvyšnými peniazmi.

PREDICATE CRIMES

„Špecifikované protiprávne činnosti“, ktorých výnosy, ak sú súčasťou predmetnej transakcie, môžu viesť k trestnému stíhaniu za pranie špinavých peňazí. Väčšina predpisov proti praniu špinavých peňazí obsahuje širokú definíciu alebo zoznam takýchto základných trestných činov. Podkladové, predikatívne trestné činy sú niekedy definované vo všeobecnosti ako trestné činy alebo „všetky trestné činy v trestnom zákonníku“.

PREPAID CARD

Platobná carta s vopred nahranou hodnotou, ktorá nie je viazaná na bankový účet. Predplatené karty môžu predstavovať zvýšené riziko AML, keďže umožňujú anonymné transakcie a ľahký prevoz hodnôt. Regulácia predplatených kariet (limity, povinnosť identifikácie) je súčasťou rámca AML/CFT vo väčšine jurisdikcií. 5AMLD a 6AMLD sprísnili požiadavky v EÚ.

PRIVATE BANKING

Oddelenie finančnej inštitúcie, ktoré poskytuje špičkové služby bohatým jednotlivcom (High Net Worth Indivudals – HNWI). Transakcie privátneho bankovníctva pre oblasť AML/CFT sa zvyčajne vyznačujú dôvernosťou, zložitými dohodami o skutočnom vlastníctve, offshore investičnými nástrojmi, daňovými schránkami a službami poskytovania úverov.

V kontexte AML/CFT patrí súkromné bankovníctvo medzi najvyššie rizikové oblasti finančného sektora, a to pre kombináciu niekoľkých faktorov súčasne – vysoké objemy transakcií, kultúra dôvernosti a diskrétnosti voči klientom, komplexné vlastnícke štruktúry zahŕňajúce trusty a offshore nástroje, časté využívanie jurisdikcií s vysokou mierou utajenia a osobná povaha vzťahu medzi klientom a bankovým poradcom, ktorá môže viesť k podceňovaniu rizík a lojalite voči klientovi na úkor compliance povinností. FATF a smernice AMLD explicitne identifikujú súkromné bankovníctvo ako oblasť vyžadujúcu rozšírenú hĺbkovú previerku (EDD), a to najmä pri klientoch s politickou expozíciou (PEP) alebo klientoch z vysoko rizikových jurisdikcií. Osobitnou výzvou je identifikácia skutočného vlastníka majetku spravovaného v rámci súkromného bankovníctva – prostriedky môžu prechádzať cez viaceré trusty, holdingové spoločnosti a offshore štruktúry navrhnuté práve s cieľom skryť ich skutočného vlastníka. Historické prípady ako Panama Papers, Pandora Papers alebo škandály spojené s tzv. kleptokratmi opakovane ukázali, že súkromné bankovníctvo bolo zneužívané na správu majetku pochádzajúceho z korupcie a trestnej činnosti; práve tieto prípady viedli k výraznému sprísneniu regulačných požiadaviek na súkromné bankovníctvo vrátane povinnosti schválenia

vzťahu s PEP na úrovni vrcholového manažmentu, pravidelného prehodnocovania pôvodu majetku a priebežného monitorovania transakcií zodpovedajúceho zvýšenému rizikovému profilu klientely.

PRIVATE INVESTMENT COMPANY (PIC)

PIC, známa aj ako osobná investičná spoločnosť, je typ spoločnosti, ktorá je často založená v offshore jurisdikcii s prísnymi zákonmi o utajení na ochranu súkromia jej vlastníkov. V niektorých jurisdikciách sa medzinárodná obchodná spoločnosť alebo spoločnosť oslobodená od dane označuje ako súkromná investičná spoločnosť.

PROCEEDS

Výnosom sa rozumie akýkoľvek majetok pochádzajúci z trestného činu alebo získaný priamo alebo nepriamo jeho spáchaním.

V kontexte AML/CFT je pojem výnosy z trestnej činnosti ústredným konceptom celého právneho rámca boja proti praniu špinavých peňazí – samotný trestný čin prania špinavých peňazí je definovaný ako akékoľvek konanie smerujúce k zatajeniu, transformácii alebo legalizácii práve týchto výnosov. Zámerná šírka definície je pritom kľúčová – výnosy nezahŕňajú len priamo získaný majetok, ale aj akýkoľvek majetok, do ktorého boli tieto výnosy následne investované alebo konvertované, čím sa znemožňuje obchádzanie konfiškačných a AML/CFT opatrení jednoduchým prevodom prostriedkov do inej formy aktíva. Predikátne trestné činy generujúce výnosy podliehajúce pravidlám AML/CFT sú v jednotlivých jurisdikciách vymedzené rôzne – FATF odporúča zahrnúť minimálne 21 kategórií predikátnych trestných činov vrátane obchodovania s drogami, korupcie, podvodu, terorizmu, obchodovania s ľuďmi, daňových trestných činov a kybernetickej kriminalitý, pričom 6AMLD v EÚ harmonizovala tento zoznam na 22 kategórií pre všetky členské štáty. Pre finančné inštitúcie je pochopenie pojmu výnosy z trestnej činnosti kľúčové pri hodnotení, či konkrétna transakcia alebo obchodný vzťah môže zahŕňať nakladanie s takýmito výnosmi – a teda či vzniká povinnosť podania oznámenia o podozrivej aktivite.

PROLIFERATION FINANCING (FINANCOVANIE ŠÍRENIA ZBRANÍ HROMADNÉHO NIČENIA)

Poskytovanie finančných prostriedkov alebo finančných služieb na podporu vývoja, výroby, obstarania, držby alebo šírenia zbraní hromadného ničenia a ich nosičov. FATF rozšíril svoje odporúčania (R. 1, R. 2) na pokrytie rizík financovania proliferácie v roku 2012 a sprísnil požiadavky na hodnotenie rizík financovania proliferácie v roku 2020 (FATF Odporúčanie 1).

PROPERTY

Majetkom sa rozumie majetok každého druhu, či už hmotný alebo nehmotný, hnuteľný alebo nehnuteľný, hmotný alebo nehmotný, a právne dokumenty alebo nástroje preukazujúce vlastnícke právo alebo podiel na tomto majetku. Viď. taktiež definíciu Funds or Assets.

REAL TIME GROSS SETTLEMENT SYSTEMS (RTGS)

RTGS je systém elektronických platieb, v ktorom sa platobné transakcie medzi dvoma bankami uskutočňujú v reálnom čase a jednotlivo, a nie dávkovo na konci dňa. To znamená, že keď klient požiada svoju banku o zaslanie peňazí prijímajúcej banke prostredníctvom RTGS, prevod finančných prostriedkov sa uskutoční okamžite. To je v kontraste s neokamžitými platobnými metódami, ako sú transakcie automatizovaného zúčtovacieho centra (ACH), ktoré sa spracúvajú v dávkach a ich zúčtovanie často trvá niekoľko dní. Systémy RTGS sú zvyčajne spravované na národnej úrovni centrálnou bankou krajiny. Sú obmedzené na transakcie medzi účastníkmi v rámci krajiny centrálnej banky. RTGS je zvyčajne vyhradený pre väčšie sumy transakcií, pri ktorých je dôležité previesť prostriedky rýchlo. Dostupnosť služby pre špecifické typy klientov závisí aj od krajiny.

REASONABLE APPROACH

Pojem primerané opatrenia znamená primerané opatrenia, ktoré sú primerané rizikám prania špinavých peňazí alebo financovania terorizmu – nie nadmerne zaťažujúce tam, kde je riziko nízke, a dostatočne robustné tam, kde je riziko vysoké.

V kontexte AML/CFT je primeraný prístup priamym vyjadrením prístupu založeného na riziku (risk-based approach), ktorý je základným pilierom odporúčaní FATF a smerníc AMLD – regulačný rámec zámerne nestanovuje jednotné rigidné požiadavky pre všetky situácie, ale vyžaduje, aby inštitúcie samy posúdili riziká a navrhli opatrenia zodpovedajúce ich povahe, rozsahu a intenzite. Primeranosť opatrení sa posudzuje v dvoch smeroch súčasne – opatrenia musia byť dostatočné na účinné zmiernenie identifikovaných rizík, čo vylučuje formálny súlad bez skutočnej účinnosti, ale zároveň nesmú byť neprimerane zaťažujúce pre klientov a inštitúciu tam, kde to riziková situácia nevyžaduje, čo je priamou reakciou na problém de-riskingu a finančného vylúčenia. Pre finančné inštitúcie má primeraný prístup praktický dopad na každodennú compliance prax – odôvodňuje rozdielnu intenzitu hĺbkovej previerky pri rôznych klientoch, flexibilitu pri nastavovaní prahových hodnôt monitorovacích systémov a možnosť zohľadniť špecifické okolnosti konkrétneho obchodného vzťahu; regulátori pri dohľadových inšpekciách posudzujú, či inštitúcia dokáže preukázať, že jej opatrenia sú skutočne primerané identifikovaným rizikám, a nie len mechanicky aplikované bez ohľadu na konkrétny kontext.

REASONABLE CAUSE (TO SUSPECT)

V Spojenom kráľovstve musí mať firma pri absencii jednoznačnej vedomosti o protiprávnom konaní dôvodné podozrenie, že má v držbe alebo kontroluje hospodárske aktíva určenej osoby. Dôvodné podozrenie je definované ako súbor okolností, z ktorých by čestná a rozumná osoba mala vyvodiť vedomosť alebo si vytvoriť podozrenie z protiprávneho konania.

V kontexte AML/CFT je pojem dôvodného podozrenia zásadný, keďže priamo určuje prah, pri ktorého prekročení vzniká povinnosť podať oznámenie o podozrivej aktivite (SAR/STR) – a teda aj zodpovednosť zamestnancov a inštitúcie v prípade jeho nesplnenia. Štandard čestnej a rozumnej osoby je objektívny, nie subjektívny – nestačí, že konkrétny zamestnanec osobne nepojal podozrenie, ak by ho za rovnakých okolností pojala rozumná a skúsená osoba na jeho mieste. Tento princíp má niekoľko dôležitých praktických dôsledkov: prah pre podanie SAR/STR je nižší ako štandard dôkazu vyžadovaný v trestnom konaní, zamestnanci sú povinní aktívne vyhodnocovať dostupné informácie a nie pasívne čakať na jednoznačný dôkaz protiprávnosti, inštitúcie sú povinné vzdelávať zamestnancov v rozpoznávaní okolností zakladajúcich dôvodné podozrenie a zdokumentovanie procesu vyhodnocovania podozrenia je nevyhnutné na preukázanie, že inštitúcia konala v súlade s týmto štandardom. Regulátori a súdy pri posudzovaní prípadov nedbalostného nepodania SAR/STR hodnotia, či okolnosti boli také, že by rozumná a skúsená compliance osoba podozrenie pojala – a ak áno, absencia podania oznámenia zakladá právnu zodpovednosť inštitúcie.

RED FLAG

Varovný signál, ktorý by mal upozorniť na potenciálne podozrivú situáciu, transakciu alebo činnosť.

REGISTER, CORPORATE

Firemný alebo obchodný register je zoznam kľúčových informácií o spoločnosti, napríklad kedy bola spoločnosť založená a kto sú jej vlastníci a riaditelia. Korporátne (alebo podnikové) registre sú často verejne dostupné na webovej stránke spoločnosti alebo na webových stránkach spravovaných profesijnými združeniami alebo subjektmi, ako sú obchodné komory alebo právne databázy.

REGTECH (REGULATORY TECHNOLOGY)

Technológie, ktoré finančným inštitúciám pomáhajú efektívnejšie plniť regulačné požiadavky vrátane AML/CFT. RegTech riešenia zahŕňajú automatizovaný transakčný monitoring, AI-driven screening sankcií, digitálnu onboarding a KYC, hodnotenie rizík a regulačné reportovanie. Regulátori vrátane EBA a FATF podporujú zodpovedné používanie RegTech pri zachovaní efektívnosti kontroloného systému.

REGULATORY AGENCY

Vládny subjekt zodpovedný za dohľad nad jednou alebo viacerými kategóriami finančných inštitúcií. Agentúra má vo všeobecnosti právomoc vydávať nariadenia, vykonávať kontroly, ukladať pokuty a sankcie, obmedzovať činnosti a niekedy aj ukončiť štatúty inštitúcií, ktoré patria do jej právomoci. Väčšina finančných regulačných agentúr zohráva významnú úlohu pri prevencii a odhaľovaní prania špinavých peňazí a iných finančných trestných činov. Väčšina regulačných orgánov sa zameriava na domáce inštitúcie, ale niektoré majú možnosť regulovať zahraničné pobočky a operácie inštitúcií.

RELATIVES AND CLOSE ASSOCIATES (RCA)

Osoby alebo podniky, ktoré sú nejakým spôsobom prepojené alebo majú blízky vzťah s politicky exponovanou osobou (PEP). Ich blízky vzťah k PEP ich automaticky robí zraniteľnými voči finančným trestným činom, ktoré slúžia na pranie špinavých peňazí, ako je korupcia, úplatkárstvo alebo zneužitie moci. Preto sú monitorovaní, aby dodržiavali predpisy proti praniu špinavých peňazí (AML).

REMITTANCE SERVICES

Remitenčné služby, označované aj ako žírové domy alebo casas de cambio, sú podniky, ktoré prijímajú hotovosť alebo iné finančné prostriedky, ktoré prostredníctvom bankového systému prevádzajú na iný účet. Účet vedie pridružená spoločnosť v zahraničnej jurisdikcii, kde sú peniaze sprístupnené konečnému príjemcovi.

REPORTING REQUIREMENTS, INITIAL AND PERIODIC

Počiatočné a pravidelné vykazovanie často existujú vedľa seba. K počiatočnému hláseniu dochádza okamžite po identifikácii finančných prostriedkov a aktivácii zmrazenia alebo zamietnutia; toto hlásenie zvyčajne zahŕňa poskytnutie podrobného rozpisu expozície finančnej inštitúcie voči cieľu sankcií regulačnému orgánu. Okrem toho mnohé jurisdikcie vyžadujú od finančnej inštitúcie ročné (ako v prípade OFAC) alebo štvrťročné správy o zablokovaných aktívach. Tieto správy poskytujú prehľad aktív, ktoré firma drží v súlade s konkrétnymi sankčnými obmedzeniami, a spôsob, akým boli aktíva oddelené.

REPUTATIONAL RISK

Možnosť, že nepriaznivá publicita týkajúca sa obchodných postupov a združení finančnej inštitúcie, či už presná alebo nie, spôsobí stratu dôvery v integritu inštitúcie. Banky a iné finančné inštitúcie sú obzvlášť zraniteľné voči reputačnému riziku, pretože sa môžu stať nástrojom alebo obeťou nezákonných činností páchaných klientmi. Takéto inštitúcie sa môžu chrániť prostredníctvom programov Poznaj svojho zákazníka a Poznaj svojho zamestnanca.

RESPONDENT BANK

Banka, pre ktorú iná finančná inštitúcia zriaďuje, vedie, spravuje alebo spravuje korešpondenčný účet. Termín korešpondenčná banka označuje finančnú inštitúciu, ktorá poskytuje služby inej finančnej inštitúcii - zvyčajne v inej krajine. Pôsobí ako sprostredkovateľ alebo agent, ktorý uľahčuje bankové prevody, vykonáva obchodné transakcie, prijíma vklady a zhromažďuje dokumenty v mene inej banky. Korešpondenčné banky s najväčšou pravdepodobnosťou využívajú domáce banky na obsluhu transakcií, ktoré buď vznikajú, alebo sú ukončené v zahraničí. Domáce banky vo všeobecnosti využívajú korešpondenčné banky na získanie prístupu na zahraničné finančné trhy a na obsluhu medzinárodných klientov bez toho, aby museli otvárať pobočky v zahraničí.

RISK APPETITE

Miera rizika, ktorú je firma ochotná prijať pri hľadaní hodnoty alebo príležitosti. Rizikový apetít firmy odráža jej filozofiu riadenia rizík a úroveň komfortu pri podnikaní v situáciách, v ktorých by mohlo existovať zvýšené riziko sankcií. Ochota podstupovať riziko ovplyvňuje kultúru a štýl fungovania firmy a riadi prideľovanie zdrojov. Rizikový apetít organizácie sa určuje prostredníctvom procesu hodnotenia rizík a formalizuje sa vo vyhlásení o rizikovom apetíte alebo v rámci. Podnik by mal určiť svoj rizikový apetít na základe zdrojov, ktoré môže investovať do kontrol, personálu a opatrení na ochranu svojej povesti. Firmy môžu mať zastrešujúci rizikový apetít (t. j. celopodnikový) a/alebo môžu mať rizikový apetít definovaný na podrobnejšej úrovni (napr. podľa oddelení).

RISK ASSESSMENT

Nástroj, ktorý umožňuje podniku identifikovať a posúdiť rozsah, v akom môže byť vystavený rizikám. V globálnom bankovníctve tvorí hodnotenie rizík základ spoľahlivého programu dodržiavania sankcií. Hlavným účelom hodnotenia rizík je podporiť zlepšenie riadenia rizík finančnej kriminality prostredníctvom identifikácie všeobecných a špecifických sankčných rizík, ktorým finančná inštitúcia čelí; spôsobov, akými sú tieto riziká zmierňované kontrolnými mechanizmami programu dodržiavania sankcií firmy; a akýchkoľvek ďalších kontrolných mechanizmov na zmiernenie zostatkového rizika, ktoré inštitúcii zostáva. Dobre naplánované a dobre sformulované hodnotenie rizík umožňuje podniku pochopiť svoj rizikový profil a následne určiť svoju ochotu podstupovať riziká v situáciách, v ktorých by mohlo existovať zvýšené riziko sankcií.

RISK-BASED APPROACH

Posúdenie rôznych rizík spojených s rôznymi typmi podnikov, klientov, účtov a transakcií s cieľom maximalizovať účinnosť programu proti praniu špinavých peňazí.

V kontexte AML/CFT predstavuje prístup založený na riziku fundamentálny posun od predchádzajúceho preskriptívneho prístupu – namiesto jednotných pravidiel aplikovaných rovnako na všetkých klientov a transakcie bez ohľadu na ich rizikovosť umožňuje RBA inštitúciám koncentrovať zdroje, pozornosť a kontrolné mechanizmy tam, kde je riziko najvyššie. FATF zakotvil RBA ako ústredný princíp svojich odporúčaní pri ich revízii v roku 2012 a odvtedy je základom AML/CFT regulácie na globálnej úrovni. Implementácia RBA prebieha na troch úrovniach – na národnej úrovni prostredníctvom národného hodnotenia rizík (NRA) identifikujúceho kľúčové hrozby a zraniteľnosti krajiny, na sektorovej úrovni prostredníctvom hodnotení rizík vydávaných regulátormi pre konkrétne sektory a na úrovni inštitúcie prostredníctvom vlastného hodnotenia rizík zohľadňujúceho špecifiká jej klientskej základne, produktového portfólia, geografického pôsobenia a distribučných kanálov. Kľúčovými výhodami RBA sú efektívnejšie využívanie zdrojov, lepšia schopnosť reagovať na nové a vznikajúce riziká a zníženie neprimeranej záťaže pre nízkorizikových klientov; jeho hlavnou výzvou je závislosť od kvality hodnotenia rizík – podhodnotenie rizika vedie k nedostatočným kontrolám, zatiaľ čo nadhodnotenie vedie k de-riskingu a finančnému vylúčeniu. Regulátori pri dohľadových inšpekciách posudzujú, či inštitúcia skutočne aplikuje RBA v praxi alebo len formálne deklaruje jeho využívanie bez toho, aby sa intenzita kontrol skutočne líšila v závislosti od rizikovosti klienta alebo transakcie.

ROMANIZATION

Proces preberania iného systému písania (t. j. systému, ktorý často nepoužíva latinskú abecedu A-Z) a jeho prevodu do latinky - t. j. prevod písma do písma, ktorým sa dnes píšu jazyky, ako je angličtina. Niektoré písma nemajú

ekvivalentné písmená alebo symboly; v dôsledku toho môžu existovať rozdiely v písaní mien a slov, aj keď sú napísané štandardnou abecedou.

QUALIFYING WIRE TRANSFERS

Znamená cezhraničný bankový prevod nad stanovenú hranicu, ako je opísaná v odseku 5 výkladovej poznámky k odporúčaniu 16 (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 16).

SANCTION SCREENING

Proces automatizovaného alebo manuálneho porovnávania zákazníkov, protistrán a transakcií so sankčnými zoznamami vydanými medzinárodnými organizáciami (OSN), EÚ, USA (OFAC), UK (OFSI) a inými jurisdikciami. Cieľom je identifikovať a blokovať zakázané transakcie a zabrániť obchodným vzťahom so sankcionovanými subjektami.

SATISFIED

Ak sa v odporúčaniach FATF odkazuje na to, že finančná inštitúcia je v danej veci spokojná, musí byť schopná odôvodniť svoje posúdenie príslušným orgánom.

V kontexte AML/CFT má pojem „satisfied“ v odporúčaniach FATF špecifický a záväzný obsah – nejde o subjektívny pocit spokojnosti, ale o zdokumentované a odôvodnené rozhodnutie, ktoré obstojí pri objektívnom preskúmaní príslušným orgánom. Tento koncept sa objavuje v kľúčových bodoch AML/CFT procesu, napríklad pri rozhodovaní o primeranosti vykonanej hĺbkovej previerky, pri posudzovaní, či pôvod majetku klienta bol dostatočne overený, alebo pri hodnotení, či obchodný vzťah môže pokračovať napriek identifikovaným rizikovým faktorom. Praktický dopad tohto princípu je zásadný – inštitúcia nemôže jednoducho konštatovať, že je spokojná s výsledkom due diligence bez toho, aby vedela preukázať, aké konkrétne kroky podnikla, aké informácie získala, ako ich vyhodnotila a prečo dospela k danému záveru. Regulátori a orgány činné v trestnom konaní pri posudzovaní prípadov AML/CFT zlyhaní skúmajú práve túto dokumentačnú stopu – či inštitúcia mala skutočný a odôvodnený základ pre svoje rozhodnutia, alebo len formálne deklarovala spokojnosť bez skutočného posúdenia rizík; absencia zdokumentovaného odôvodnenia je sama osebe považovaná za nedostatok AML/CFT programu bez ohľadu na to, či samotné rozhodnutie bolo vecne správne.

SAFE HARBOR

Právna ochrana finančných inštitúcií, ich riaditeľov, vedúcich pracovníkov a zamestnancov pred trestnoprávnou a občianskoprávnou zodpovednosťou za porušenie akýchkoľvek obmedzení týkajúcich sa poskytovania informácií stanovených zmluvou alebo akýmkoľvek legislatívnym, regulačným alebo administratívnym zákazom, ak v dobrej viere nahlásia svoje podozrenia jednotke finančného vyšetrovania (FIU), a to aj v prípade, že presne nevedeli, o akú trestnú činnosť ide, a bez ohľadu na to, či k nezákonnej činnosti skutočne došlo.

SANCTIONS

Sankcie sú trestné alebo reštriktívne opatrenia, ktoré prijímajú jednotlivé krajiny, režimy alebo koalície s primárnym cieľom vyvolať zmenu správania alebo politiky. Sankcie môžu obmedzovať obchod, finančné transakcie, diplomatické vzťahy a pohyb. Môžu byť špecifické alebo všeobecné, pokiaľ ide o ich vykonávanie a presadzovanie. Sankcie sa označujú aj ako reštriktívne opatrenia.

SANCTIONS COMPLIANCE

Dodržiavanie právnych predpisov, nariadení, pravidiel a noriem súvisiacich so sankciami, ktoré tvoria komplexné sankčné prostredie.

SANCTIONS COMPLIANCE OFFICER (SCO)

V rámci druhej línie obrany v štruktúre riadenia programu dodržiavania sankcií je SCO zodpovedný za priebežné monitorovanie dodržiavania sankcií vrátane testovania vzoriek a preskúmania správ o výnimkách, aby bolo možné eskalovať zistené nedodržiavanie alebo iné problémy na vrcholový manažment a prípadne na predstavenstvo. SCO je kontaktným miestom pre všetky otázky týkajúce sa sankcií pre interné a externé orgány a zodpovedá za nahlasovanie podozrivých transakcií. Na umožnenie úspešného dohľadu nad programom dodržiavania sankcií musí byť SCO dostatočne nezávislý od obchodných línií, aby sa predišlo konfliktu záujmov a nestrannému poradenstvu a konzultáciám.

SANCTIONS COMPLIANCE PROGRAM (SCP)

Program, ktorý firma realizuje s cieľom splniť očakávania regulačného orgánu týkajúce sa dodržiavania sankcií a riadiť sankčné riziko firmy. OFAC nabáda organizácie podliehajúce jurisdikcii USA, aby pri dodržiavaní sankcií uplatňovali prístup založený na riziku, a to prostredníctvom vypracovania, implementácie a pravidelnej aktualizácie SCP. SCP sa riadia podobnou metodikou, akú prijímajú programy na zabezpečenie súladu s predpismi proti praniu špinavých peňazí. Podľa OFAC päť základných zložiek SCP sú: 1) záväzok manažmentu; 2) hodnotenie rizík; 3) vnútorné kontroly; 4) testovanie a audit; a 5) školenie.

SANCTIONS EVASION

Úmyselná snaha odstrániť alebo zakryť účasť sankcionovaných miest, subjektov alebo jednotlivcov na transakcii alebo sérii transakcií. Keď sa obchádzanie sankcií podarí, obchod, ktorý by bol označený, zdanený, obmedzený alebo zakázaný, môže bez prekážok pokračovať.

SANCTIONS DUE DILIGENCE (SDD)

Proces podobný procesu Poznaj svojho klienta (KYC) / povinnej starostlivosti vo vzťahu ku klientovi (CDD), ktorý sa zameriava na riziká špecifické pre sankcie a zohľadňuje riadenie a hodnotenie rizík. SDD vychádza z informácií KYC/CDD, ktoré organizácia zhromažďuje v rámci existujúceho programu AML. SDD sa uplatňuje počas celého životného cyklu vzťahu na začiatku vzťahu (t. j. pri vstupe do vzťahu); pri zavádzaní nových produktov, ako reakcia na spúšťacie udalosti počas vzťahu, ako je napríklad „zhoda“ vygenerovaná skríningovým nástrojom; počas pravidelných preskúmaní a pri ukončení vzťahu.

SANCTIONS LIST

Dokument alebo databáza obsahujúca zoznam fyzických a právnických osôb a krajín, s ktorými je nezákonné obchodovať.

SANCTIONS REGIME

Súbor sankcií, ktoré majú spoločnú súvislosť alebo tému. Označujú sa buď podľa vydavateľa súboru sankcií, alebo podľa zamýšľaného účelu súboru sankcií. Napríklad „sankčný režim OFAC“ alebo „sankčný režim voči Severnej Kórei“. V závislosti od kontextu môže byť režim sankcií obmedzený na jednostranné sankcie alebo môže zahŕňať mnohostranné sankcie.

SCOPE OF LICENSING

Podrobnosti o tom, ktoré činnosti sú v rámci danej licencie povolené. Ak napríklad firma spravuje zmrazený majetok klienta a potrebuje previesť časť majetku klienta na podnik (napríklad na veriteľa s oprávnenou pohľadávkou), musí zistiť, či a za akých okolností licencia túto činnosť umožňuje.

SCOPE OF PERMITTED ACTIVITIES

Podrobnosti o tom, ktoré činnosti sú povolené bez licencie na základe sankcie a ktoré sú povolené len s licenciou. V licencii môže byť

stanovené, že určité činnosti sú povolené len počas určitého obdobia alebo v určitých ročných obdobiach.

SECOND LINE OF DEFENSE

Funkcia dodržiavania sankcií, väčšia funkcia dodržiavania predpisov a oddelenia ľudských zdrojov a technológií tvoria druhú líniu obrany v rámci štruktúry riadenia programu dodržiavania sankcií. Pracovník zodpovedný za dodržiavanie sankcií zabezpečuje priebežné monitorovanie dodržiavania sankcií s cieľom umožniť eskaláciu zistených problémov. Vo všeobecnosti druhá línia existuje na zabezpečenie toho, aby postupy a procesy SDD uplatňované prvou líniou boli správne navrhnuté, pevne zavedené a uplatňované tak, ako bolo zamýšľané. Druhá línia obrany skúma účinnosť kontrolných mechanizmov používaných na zmiernenie sankčných rizík; poskytuje informácie prvej línii a vyšetruje možné nedodržiavanie sankčných obmedzení.

SECONDARY SANCTIONS

Sankcie, ktoré cieľa na subjekty tretích krajín obchodujúce so sankcionovanou krajinou alebo osobami, aj keď sami nie sú priamo cieľom primárnych sankcií. Sekundárne sankcie, ktoré primárne využívajú USA, vytvárajú extrateritoriálne sankčné riziko pre medzinárodné finančné inštitúcie a vyžadujú osobitné zohľadnenie v rámci screeningových a compliance programov.

SECTORAL SANCTION

Novšia forma obmedzenia zameraná na kľúčové subjekty a odvetvia hospodárstva krajiny. Zakazujú určité typy transakcií s určitými osobami alebo subjektmi v cieľovej krajine v rámci cieľového odvetvia hospodárstva. Sektorové sankcie sú pri uplatňovaní veľmi závislé od skutočností a kontextu.

SECTORAL SANCTIONS IDENTIFICATION LIST (SSI LIST)

Zoznam osôb, na ktoré sa vzťahujú sektorové sankcie. Zoznam SSI nie je súčasťou zoznamu osobitne označených osôb (SDN). Jednotlivci a spoločnosti na zozname SSI sa však môžu objaviť aj na zozname SDN.

SEIZE

Zákaz prevodu, konverzie, disponovania alebo pohybu finančných prostriedkov alebo iných aktív na základe opatrenia iniciovaného príslušným orgánom alebo súdom v rámci mechanizmu zmrazenia. Na rozdiel od zmrazenia však zaistenie umožňuje príslušnému orgánu prevziať kontrolu nad určenými finančnými prostriedkami alebo inými aktívami. Zabavené aktíva zostávajú majetkom osoby (osôb) alebo subjektu (subjektov), ktoré o ne mali záujem v čase zabavenia, hoci príslušný orgán často prevezme držbu, správu alebo riadenie zabavených aktív.

SELF-REGULATORY BODY (SRB)

SRB je orgán, ktorý zastupuje určitú profesiu (napr. advokáti, notári, iní nezávislí právnici alebo účtovníci) a ktorý sa skladá z členov tejto profesie, má úlohu regulovať osoby, ktoré sú kvalifikované na vstup do profesie a ktoré ju vykonávajú, a tiež vykonáva určité funkcie typu dohľadu alebo monitorovania. Takéto orgány by mali presadzovať pravidlá, aby sa zabezpečilo, že osoby vykonávajúce povolanie budú dodržiavať vysoké etické a morálne normy.

SENIOR FOREIGN POLITICAL FIGURE

Americký termín pre zahraničné politicky exponované osoby (PEP).

SERIAL PAYMENT

Vzťahuje sa na priamy postupný platobný reťazec, pri ktorom prevod a sprievodná platobná správa putujú spoločne z finančnej inštitúcie príkazcu do finančnej inštitúcie príjemcu priamo alebo prostredníctvom jednej alebo viacerých sprostredkujúcich finančných inštitúcií (napr. korešpondenčných bánk) (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 16).

SETTLORS

Osoby alebo spoločnosti, ktoré prevedú vlastníctvo svojho majetku na správcov prostredníctvom zvereneckej zmluvy. Ak majú správcovia určitú voľnosť pri investovaní a rozdeľovaní majetku zvereneckého fondu, môže byť k listine pripojený právne nezáväzný list, v ktorom sa uvádza, čo si zriaďovateľ želá, aby sa s majetkom urobilo.

SHAM DIVESTMENT

Transakcia, pri ktorej cieľ sankcií predáva aktíva alebo vlastný kapitál blízkym spolupracovníkom alebo iným spriazneným osobám. Môžu to byť priatelia, kolegovia, podriadení, obchodní partneri a rodinní príslušníci. Podobne ako pri použití izolovanej spoločnosti ide o to, že cieľ sankcií už zdanlivo „nevlastní“ aktíva alebo akcie spoločnosti. Cieľová osoba však naďalej ovplyvňuje alebo kontroluje majetok alebo činnosť spoločnosti.

SHANGHAI COOPERATION ORGANIZATION (SCO)

Šanghajská organizácia pre spoluprácu - medzivládna vzájomná bezpečnostná organizácia, ktorú v roku 2001 v Šanghaji založili vedúci predstavitelia Číny, Kazachstanu, Kirgizska, Ruska, Tadžikistanu a Uzbekistanu. Jej hlavnými cieľmi sú zaistenie bezpečnosti a stability, boj proti terorizmu, separatizmu, extrémizmu a obchodu s drogami a rozvoj hospodárskej spolupráce, ako aj vedeckej a kultúrnej výmeny medzi členskými štátmi.

SHELF COMPANY

Spoločnosť, ktorá bola založená mesiace alebo roky vopred, často právnickou alebo účtovníckou firmou. Potom sa spoločnosť „odloží“, kým nie je potrebná. Niektorí investori využívajú tieto „shelf“ spoločnosti alebo „staršie“ spoločnosti, aby získali čistý obchodný záznam.

SHELL BANK

Banka, ktorá existuje len na papieri a ktorá nie je fyzicky prítomná v krajine, kde je registrovaná alebo licencovaná, a ktorá nie je prepojená s regulovanou skupinou finančných služieb, ktorá podlieha účinnému konsolidovanému dohľadu.

SHELL COMPANY

Spoločnosť bez aktívnej činnosti alebo významného majetku. Krycie spoločnosti sú legálne, ale ľudia ich niekedy používajú nelegálne - napríklad na zakrytie vlastníctva podniku.

SHOULD

Na účely posúdenia súladu s odporúčaniami FATF má slovo „mal by“ rovnaký význam ako „musí/je povinný“.

SIMPLE CHECKS

Jednoduché kontroly sú jedným z prvých krokov pri vyšetrovaní a predstavujú prvotné kroky, ktoré sa vykonávajú s cieľom vylúčiť alebo potvrdiť súvislosť so sankciami; príkladom jednoduchej kontroly je porovnanie

údajov o sankcionovanom subjekte s údajmi spoločnosti Know Your Customer (KYC).

SIMPLIFIED DUE DILIGENCE (SDD)

Zjednodušená hĺbková previerka zákazníka aplikovateľná na zákazníkov, produkty alebo transakcie, pri ktorých je riziko prania špinavých peňazí a financovania terorizmu preukázateľne nízke. SDD zahŕňa menej prísne opatrenia na identifikáciu a overenie zákazníka v porovnaní so štandardnou CDD. Podmienky uplatňovania SDD sú stanovené v národnej legislatíve AML/CFT a musia byť odôvodnené hodnotením rizík.

SMURFING

Bežne používaná metóda prania špinavých peňazí, tzv. smurfing, spočíva vo využívaní viacerých osôb a/alebo viacerých transakcií pri vkladoch hotovosti, nákupe peňažných nástrojov alebo bankových zmeniek v sumách, ktoré nedosahujú prah pre vykazovanie. Osoby najaté na vykonávanie transakcií sa označujú ako „šmudlovia“. Pozri štruktúrovanie

SOURCE OF FUNDS/SOURCE OF WEALTH

Pôvod finančných prostriedkov (SoF) označuje zdroj konkrétnych finančných prostriedkov použitých pri transakcii alebo v obchodnom vzťahu. Pôvod majetku (SoW) označuje spôsob, akým osoba nadobudla celkový majetok. Oba pojmy sú kľúčovými prvkami hĺbkovej previerky, najmä pri PEP a zákazníkoch s vysokým rizikom, a pomáhajú identifikovať potenciálne pranie špinavých peňazí.

SOURCES, PRIMARY

Zdroje informácií, ktoré poskytujú priame dôkazy o sankcii alebo cieli sankcie. Medzi primárne zdroje patria napríklad sankčné nástroje, sankčné zoznamy, zoznamy obchodných aktivít a transakčné aktivity.

SOURCES, SECONDARY

Zdroje vytvorené „dodatočne“, ktoré podávajú správu, analyzujú alebo zhromažďujú informácie, ktoré sa už objavili v primárnych dokumentoch. Ak existuje rozpor medzi primárnymi zdrojmi a sekundárnymi zdrojmi, je to červená vlajka, ktorá si zaslúži minimálne ďalšie skúmanie s cieľom objasniť rozpor. Príkladom sekundárnych zdrojov sú podnikové registre, databázy tretích strán a mediálne publikácie.

SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS LIST (SDN LIST)

Zoznam osôb a spoločností, ktoré vlastní, kontroluje alebo koná v mene cieľovej krajiny, zverejnený OFAC. Zoznam obsahuje aj skupiny a osoby, ako sú teroristi alebo obchodníci s drogami, ktoré sú spojené s konkrétnym trestným činom, a nie s krajinou. Zoznam vedie ministerstvo financií USA, ktoré môže osobu alebo spoločnosť označiť za SDN. Ak vláda označí osobu alebo spoločnosť za SDN, zablokuje ich aktíva a zakáže osobám z USA s nimi obchodovať. Vláda môže tiež uložiť pokuty a uväzniť porušovateľov zákona. Jednotlivci tiež môžu prísť o svoje vývozné privilégiá. Vláda USA môže osobu alebo podnik zaradiť na zoznam blokovaných, odmietnutých alebo vylúčených osôb a inštitúcií.

STING OPERATION

Vyšetrovacia taktika, pri ktorej sa tajní policajti vydávajú za zločincov, niekedy prostredníctvom „krycieho“ podniku, aby získali dôveru podozrivých alebo známych zločincov s cieľom získať informácie a dôkazy o trestnej činnosti. Je to účinný prostriedok na identifikáciu zločincov, preniknutie do zločineckých organizácií a identifikáciu znehodnoteného majetku v prípadoch prania špinavých peňazí a iných prípadoch.

STRAIGHT-THROUGH PROCESSING

Priame spracovanie je automatizovaný proces vykonávaný výlučne prostredníctvom elektronických prevodov bez manuálneho zásahu. Obľúbené je jeho použitie pri spracovaní platieb, ako aj pri spracovaní obchodov s cennými papiermi. Každá spoločnosť, ktorá sa zaoberá priamym spracovaním, musí mať zavedené potrebné systémy a technické siete, ktoré uľahčujú efektívnosť STP. STP sa vzťahuje na platobné transakcie, ktoré sa vykonávajú elektronicky bez potreby manuálneho zásahu (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 16).

STRAW MAN

Nesankcionovaná osoba s nízkym verejným profilom, ktorá koná v mene alebo na mieste sankcionovaného subjektu, nazývaná aj „nastrčená osoba“. Slamový muž/Biely kôň nevystupuje v žiadnom skutočnom zmysle ako vlastník alebo kontrolór. Namiesto toho vykonáva činnosti na pokyn sankcionovaného subjektu, ktorý je aktívny v pozadí.

STRICT LIABILITY

Zásada, že organizácia je zodpovedná, aj keď nemala v úmysle porušiť alebo vedome porušila sankciu. Organizácie sú zodpovedné aj vtedy, ak majú zavedené spoľahlivé programy dodržiavania sankcií.

STRING MATCHING

Algoritmus na efektívne vyhľadávanie, ktorý zahŕňa hľadanie výskytu vzorového reťazca v inom reťazci alebo texte. Táto metóda, označovaná aj ako porovnávanie vzorov, sa môže použiť na rozpoznávanie čísel sociálneho poistenia, telefónnych čísel, poštových smerovacích čísel a akýchkoľvek iných informácií, ktoré sa riadia špecifickým vzorom. Je tiež užitočná na hľadanie informácií, ktoré nasledujú za vedúcim textom, a následné extrahovanie textu, ktorý nasleduje za ním, ako aj na opätovné spracovanie dokumentov. Tento algoritmus funguje tak, že číta textové reťazce a porovnáva ich so vzormi.

STRIPPING

Vymazanie zahŕňa vynechanie alebo odstránenie kľúčových informácií, ako je meno odosielateľa alebo názov firmy, z platobnej správy, aby sa zabránilo ich odhaleniu. Môže k nemu dôjsť s vedomím alebo bez vedomia ostatných účastníkov transakcie. Keď bankový prevod prechádza cez viacero strán, kým sa dostane do zamýšľaného konečného cieľa, existuje viacero možností, ako skrátiť, vynechať alebo zmeniť informácie. Z tohto dôvodu väčšina jurisdikcií prijala zákony, ktoré vyžadujú, aby platby obsahovali určité „základné“ informácie vrátane mena a adresy odosielateľa a príjemcu. Ak prevod pochádza od subjektu alebo z miesta, na ktoré sa vzťahujú sankcie, a jeho zámerom je doručiť ho v rámci Spojených štátov alebo Európskej únie, kde by obmedzenia bežne platbu označili a zablokovali, osoby, ktoré sa vyhýbajú sankciám, majú motiváciu odstrániť informácie, ktoré by systém zablokovali.

STRUCTURING

Nezákonné rozdelenie hotovostných vkladov alebo výberov na menšie sumy alebo nákup peňažných nástrojov s cieľom neprekročiť prah pre vykazovanie meny. Tento postup môže zahŕňať rozdelenie peňažnej sumy na menšie množstvá a uskutočnenie dvoch alebo viacerých vkladov alebo výberov, ktoré sa dopočítajú do pôvodnej sumy. Pranie špinavých peňazí využíva štruktúrovanie na to, aby sa finančná inštitúcia vyhla podaniu hlásenia. Táto technika je bežná v jurisdikciách, ktoré majú povinné ohlasovacie povinnosti v oblasti devíz. Pozri Smurfing.

SUPERVISORS

Orgánmi dohľadu sa rozumejú určené príslušné orgány alebo neverejné subjekty, ktorých úlohou je zabezpečiť, aby finančné inštitúcie („orgány

finančného dohľadu „1) a/alebo DNFBP dodržiavali požiadavky na boj proti praniu špinavých peňazí a financovaniu terorizmu. Neverejné orgány (ktoré by mohli zahŕňať určité typy SRB) by mali mať právomoc vykonávať dohľad nad finančnými inštitúciami alebo DNFBP a ukladať im sankcie v súvislosti s požiadavkami na boj proti praniu špinavých peňazí a financovaniu terorizmu. Tieto neverejné orgány by tiež mali byť zákonom splnomocnené na výkon funkcií, ktoré vykonávajú, a mali by byť pod dohľadom príslušného orgánu v súvislosti s týmito funkciami.

SUBPOENA

Povinné súdne konanie, ktoré vydáva súd s cieľom prinútiť svedka dostaviť sa na súdne konanie, pričom niekedy sa vyžaduje, aby svedok priniesol určité dokumenty. Tento pojem sa môže vzťahovať buď na proces, alebo na samotný dokument, ktorý núti príjemcu konať.

SUSPICIOUS ACTIVITY REPORT (SAR)

V prípade podozrenia z prania špinavých peňazí finančné inštitúcie a iné orgány, na ktoré sa vzťahujú predpisy o praní špinavých peňazí. Tie tiež predkladajú FIU správy týkajúce sa podozrivých činností. Preto sa tieto správy nazývajú SAR.

SUSPICIOUS TRANSACTION REPORT (STR)

Vládne podanie, ktoré vyžadujú vykazujúce subjekty a ktoré obsahuje účet finančnej inštitúcie o spornej transakcii. Mnohé jurisdikcie vyžadujú, aby finančné inštitúcie oznamovali podozrivé transakcie príslušným vládnym orgánom, ako je napríklad ich finančná spravodajská jednotka, na základe správy o podozrivej transakcii (STR), známej aj ako správa o podozrivej činnosti alebo SAR.

SWIFT MESSAGE

SWIFT (Society for Worldwide Interbank Financial Telecommunications) poskytuje sieť správ, ktorú finančné inštitúcie používajú na bezpečný prenos informácií a pokynov. Sieť funguje prostredníctvom štandardizovaného systému kódov, v ktorom má každá členská organizácia pridelený jedinečný kód, ktorý má 8 alebo 11 znakov. Systém správ SWIFT zasiela platobné príkazy, ktoré sa musia vyrovnať prostredníctvom korešpondenčných účtov, ktoré majú členské inštitúcie medzi sebou.

TARGET MATCH

Identifikácia strany ako strany, ktorá sa zhoduje so stranou uvedenou na sankčnom zozname. Označuje sa aj ako skutočná zhoda a je výsledkom kontroly sankcií.

TARGETED SANCTIONS

Sankcie proti konkrétnemu cieľu, spravidla s cieľom dosiahnuť konkrétny výsledok. Cielené sankcie môžu mať podobu finančných alebo obchodných obmedzení zameraných na obmedzenie pohybu a môže ich jednostranne uplatňovať jedna krajina alebo mnoho krajín. Cielené sankcie sa označujú aj ako inteligentné sankcie.

TAX HAVEN

Krajiny, ktoré ponúkajú zahraničným investorom a vkladateľom osobitné daňové stimuly alebo vyhýbanie sa daňovým povinnostiam.

TERRORIST

Pojem terorista sa vzťahuje na každú fyzickú osobu, ktorá: (i) pácha alebo sa pokúša spáchať teroristické činy akýmikoľvek prostriedkami, priamo alebo nepriamo, nezákonne a úmyselne; (ii) zúčastňuje sa ako spolupáchateľ na teroristických činoch; (iii) organizuje alebo riadi iné osoby, aby spáchali teroristické činy; alebo (iv) prispieva k spáchaniu teroristických činov skupinou osôb konajúcich so spoločným cieľom, ak je príspevok vykonaný úmyselne a s cieľom podporiť teroristický čin alebo s vedomím zámeru skupiny spáchať teroristický čin.

TERRORIST ACT

Teroristický čin zahŕňa: (a) čin, ktorý je trestným činom v rozsahu pôsobnosti a v zmysle jednej z nasledujúcich zmlúv: (i) Dohovor o potláčaní nezákonného zmocnenia sa lietadiel (1970); ii) Dohovor o potláčaní protiprávnych činov ohrozujúcich bezpečnosť civilného letectva (1971); iii) Dohovor o predchádzaní a trestaní zločinov proti medzinárodne chráneným osobám vrátane diplomatických zástupcov (1973); iv) Medzinárodný dohovor proti braniu rukojemníkov (1979); v) Dohovor o fyzickej ochrane jadrového materiálu (1980); (vi) Protokol o potláčaní protiprávnych násilných činov na letiskách slúžiacich medzinárodnému civilnému letectvu, doplňujúci Dohovor o potláčaní protiprávnych činov ohrozujúcich bezpečnosť civilného letectva (1988); vii) Dohovor o potláčaní protiprávnych činov ohrozujúcich bezpečnosť námornej plavby (2005); (viii) Protokol o potláčaní protiprávnych činov ohrozujúcich bezpečnosť pevných platforiem nachádzajúcich sa na kontinentálnom šelfe (2005); ix) Medzinárodný dohovor o potláčaní teroristických bombových útokov (1997) a x) Medzinárodný dohovor o potláčaní financovania terorizmu (1999), (b) akýkoľvek iný čin, ktorého cieľom je spôsobiť smrť alebo vážnu ujmu na zdraví civilnej osobe alebo akejkoľvek inej osobe, ktorá sa aktívne nezúčastňuje na nepriateľských akciách v situácii ozbrojeného konfliktu, ak je účelom takéhoto činu vzhľadom na jeho povahu alebo kontext zastrašiť obyvateľstvo alebo prinútiť vládu alebo medzinárodnú organizáciu, aby vykonala nejaký čin alebo sa ho zdržala.

TERRORIST FINANCING

Proces, ktorým teroristi financujú svoje operácie s cieľom vykonať teroristické činy. Existujú dva základné zdroje financovania teroristických aktivít. Prvý zahŕňa finančnú podporu od krajín, organizácií alebo jednotlivcov. Druhý zahŕňa širokú škálu činností generujúcich príjmy, z ktorých niektoré sú nezákonné, vrátane pašovania a podvodov s kreditnými kartami.

TERRORIST FINANCING ABUSE

Vzťahuje sa na využívanie neziskových organizácií teroristami a teroristickými organizáciami na získavanie alebo presun finančných prostriedkov, poskytovanie logistickej podpory, podnecovanie alebo uľahčovanie náboru teroristov alebo inú podporu teroristov alebo teroristických organizácií a operácií.

TERRORIST FINANCING CONVENTION

Medzinárodný dohovor o potláčaní financovania terorizmu 1999. Cieľom Medzinárodného dohovoru o potláčaní financovania terorizmu je posilniť medzinárodnú spoluprácu medzi štátmi pri navrhovaní a prijímaní účinných opatrení na financovania terorizmu, ako aj na jeho potláčanie prostredníctvom trestného stíhania a boja proti terorizmu a jeho páchateľom.

TERRORIST FINANCING OFFENCE

Odkazy (s výnimkou odporúčania FATF 4) na trestný čin financovania terorizmu sa vzťahujú nielen na hlavný trestný čin alebo trestné činy, ale aj na vedľajšie trestné činy.

TERRORIST ORGANIZATION

Pojem teroristická organizácia sa vzťahuje na akúkoľvek skupinu teroristov, ktorá: (i) pácha alebo sa pokúša spáchať teroristické činy akýmikoľvek prostriedkami, priamo alebo nepriamo, nezákonne a úmyselne; (ii)

zúčastňuje sa ako spolupáchateľ na teroristických činoch; (iii) organizuje alebo riadi iné osoby, aby spáchali teroristické činy; alebo (iv) prispieva k spáchaniu teroristických činov skupinou osôb konajúcich so spoločným cieľom, ak je príspevok vykonaný úmyselne a s cieľom podporiť teroristický čin alebo s vedomím zámeru skupiny spáchať teroristický čin.

TESTIMONY

Ústny prejav svedka, zvyčajne pod prísahou, ktorý opisuje skutočnosti známe svedkovi.

THIRD LINE OF DEFENSE

Treťou obrannou líniou v rámci štruktúry riadenia programu dodržiavania sankcií je vnútorný audit, ktorý zahŕňa nezávislé preskúmanie kontrol uplatňovaných prvými dvoma obrannými líniami. Nezávisle hodnotí riadenie rizík a kontrolné mechanizmy banky prostredníctvom pravidelných hodnotení vrátane primeranosti kontrolných mechanizmov banky na zmiernenie identifikovaných rizík. Hodnotí tiež účinnosť vykonávania kontrol zamestnancami, účinnosť dohľadu nad dodržiavaním predpisov a kontroly kvality a účinnosť školení.

THIRD PARTIES

Na účely odporúčaní FATF 6 a 7 pojem tretie strany zahŕňa okrem iného finančné inštitúcie a DNFBP. Pojem tretie strany znamená finančné inštitúcie alebo DNFBP, ktoré sú pod dohľadom alebo monitorovaním a ktoré spĺňajú požiadavky podľa odporúčania FATF 17 (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 17).

THRESHOLD CALIBRATION

Spôsob úpravy prahových hodnôt v rámci algoritmov v automatizovanom skríningovom nástroji tak, aby zodpovedali najväčším rizikovým oblastiam sankcií finančnej inštitúcie. Prahová hodnota sa zvyčajne opisuje ako percento a riadi generovanie výstrah. Kalibrácia prahových hodnôt odráža aktualizáciu a zmenu konfigurácie algoritmov na základe nových trendov, interných vyšetrovaní inštitúcie, externých informácií a kanálov aktivít finančnej kriminality, ktoré sa vyvíjajú a menia v čase.

TIPPING OFF

Nesprávne alebo nezákonné konanie spočívajúce v oznámení podozrivej osoby, že je predmetom hlásenia o podozrivej transakcii alebo je inak vyšetrovaná alebo stíhaná orgánmi.

TOLL GATES

Rôzne strany, ktoré tvoria platobný reťazec. Platobné správy prechádzajú cez mýtne brány a môžu sa v priebehu procesu meniť.

TRADE-BASED MONEY LAUNDERING (TBML)

Proces prania špinavých peňazí a financovania terorizmu prostredníctvom manipulácie s medzinárodnými obchodnými transakciami. Metódy TBML zahŕňajú nadhodnotenie alebo podhodnotenie faktúr, falošné popisovanie tovaru, viacnásobné fakturovanie a manipuláciu s množstvom. FATF identifikoval TBML ako jednu z hlavných techník prania špinavých peňazí spolu s hotovostnými transakciami a zneužívaním právnických osôb.

TRANSACTION MONITORING AND FILTERING PROGRAMS (TMPS)

Programy, ktoré sa od finančných inštitúcií vyžadujú podľa záverečného predpisu 504 Ministerstva finančných služieb štátu New York (DFS) na monitorovanie transakcií po ich vykonaní z hľadiska súladu so zákonom o bankovom tajomstve a zákonmi a predpismi o boji proti praniu špinavých peňazí. Zahŕňa požiadavky na nahlasovanie podozrivých činností, ako aj na monitorovanie transakcií pred ich vykonaním

TRANSLITERATION

Konverzia textu z jedného písma do iného, napríklad dokument napísaný arabskými znakmi sa konvertuje do cyriliky. Tento jav môže predstavovať problém pri kontrole názvov.

TRANSPARENCY INTERNATIONAL (TI)

Mimovládna organizácia so sídlom v Berlíne, ktorá sa venuje zvyšovaniu zodpovednosti vlád a obmedzovaniu medzinárodnej aj vnútroštátnej korupcie. TI bola založená v roku 1993 a pôsobí približne v 100 krajinách. Na svojej webovej stránke denne uverejňuje „správy o korupcii“ a ponúka archív spravodajských článkov a správ týkajúcich sa korupcie. Jej online výskumný a informačný systém o korupcii (Corruption Online Research and Information System, CORIS) je pravdepodobne najkomplexnejšou celosvetovou databázou o korupcii. TI je najznámejšia svojím každoročným indexom vnímania korupcie (Corruption Perceptions Index - CPI), ktorý hodnotí krajiny podľa vnímanej úrovne korupcie medzi verejnými činiteľmi; jej index úplatkárov (Bribe Payers Index - BPI) hodnotí popredné exportné krajiny podľa ich sklonu k úplatkárstvu. Každoročná správa TI o globálnej korupcii kombinuje CPI a BPI a hodnotí jednotlivé krajiny podľa celkovej úrovne korupcie. Zoznamy pomáhajú finančným inštitúciám určiť riziko spojené s konkrétnou jurisdikciou.

TRANSSHIPMENT

Preprava tovaru cez prechodné krajiny, niekedy zahŕňajúca preloženie z jedného plavidla na druhé, pred dosiahnutím zamýšľaného miesta určenia. K prekládke niekedy dochádza s cieľom vyhnúť sa blokádam v prístavoch vstupu pre sankčné režimy alebo skryť identitu krajiny pôvodu v mieste určenia. Niektoré vlády a subjekty prekládku zakazujú.

TRUST

Dohoda medzi vlastníkom nehnuteľnosti (zadávateľom), príjemcom a správcom nehnuteľnosti (správcom), na základe ktorej správca spravuje nehnuteľnosť v prospech príjemcu v súlade s podmienkami stanovenými zadávateľom.

TRUSTEE

Môže to byť platený profesionál alebo spoločnosť alebo neplatená osoba, ktorá drží majetok v správcovskom fonde oddelene od vlastného majetku správcu. Správca investuje a nakladá s majetkom v súlade so zriaďovacou listinou zriaďovateľa, pričom berie do úvahy všetky listy s prianiami. Pojmy trust a správca by sa mali chápať v súlade s článkom 2 Haagskeho dohovoru o rozhodnom práve pre trusty a ich uznávaní. Správcovia môžu byť profesionálni (napr. v závislosti od jurisdikcie právnik alebo správcovská spoločnosť), ak sú platení za výkon funkcie správcu v rámci svojej činnosti, alebo neprofesionálni (napr. osoba konajúca bez nároku na odmenu v mene rodiny).

TYPOLOGY

Označuje metódu prania špinavých peňazí a je to termín používaný FATF.

UNILATERAL SANCTIONS

Ide o sankcie, ktoré ukladá jedna krajina voči cieľovému subjektu. Vo všeobecnosti sa považujú za menej účinné ako multilaterálne sankcie. Napriek tomu slúžia na zameranie sa na konkrétne útočné praktiky v mene ukladajúcich krajín. Ako príklad možno uviesť Magnitského zákon, ktorý umožňuje uvalenie jednostranných globálnych sankcií na porušovateľov ľudských práv. Majetok môže byť zmrazený a páchateľom môže byť

zakázaný vstup do USA. Iný príklad sa vyskytol v 80. rokoch 20. storočia, keď Austrália autonómne zakázala dodávky uránu do Francúzska. Až na niekoľko výnimiek (napríklad Európska únia) sa tieto sankcie často označujú ako autonómne sankcie.

UNITED NATIONS (UN)

Medzinárodná organizácia založená v roku 1945 51 krajinami, ktoré sa zaviazali zachovať mier prostredníctvom spolupráce a kolektívnej bezpečnosti. Dnes sú členmi OSN takmer všetky štáty sveta. Pozri tiež Viedenský dohovor. OSN prispieva k boju proti organizovanému zločinu iniciatívami, ako je napríklad Globálny program proti praniu špinavých peňazí (GPML), ktorý je kľúčovým nástrojom Úradu OSN pre kontrolu drog a prevenciu kriminality v tejto úlohe. Prostredníctvom GPML OSN pomáha členským štátom zavádzať právne predpisy proti praniu špinavých peňazí a rozvíjať mechanizmy na boj proti tejto trestnej činnosti. Program podporuje rozvoj politiky proti praniu špinavých peňazí, monitoruje a analyzuje problémy a reakcie, zvyšuje povedomie verejnosti o praní špinavých peňazí a pôsobí ako koordinátor spoločných iniciatív proti praniu špinavých peňazí s inými medzinárodnými organizáciami.

UNITED NATIONS GENERAL ASSEMBLY (UNGA)

Valné zhromaždenie OSN - jeden z piatich hlavných orgánov OSN a jediný orgán, v ktorom majú všetky členské štáty rovnaké zastúpenie. Jeho právomocou je dohliadať na rozpočet OSN, vymenúvať nestálych členov Bezpečnostnej rady, prijímať správy z ostatných častí OSN a vydávať odporúčania vo forme rezolúcií Valného zhromaždenia.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)

Úrad OSN pre drogy a kriminalitu - agentúra OSN, ktorá vznikla v roku 1997 ako Úrad pre kontrolu drog a prevenciu kriminality spojením Medzinárodného programu OSN pre kontrolu drog (UNDCP) a Oddelenia pre prevenciu kriminality a trestné súdnictvo na Úrade OSN vo Viedni. V roku 2002 bol premenovaný na Úrad OSN pre drogy a kriminalitu.

UNITED NATIONS SECURITY COUNCIL (UNSC)

Bezpečnostná rada OSN - jeden z hlavných orgánov OSN, ktorého úlohou je udržiavať medzinárodný mier a bezpečnosť. Medzi jej právomoci uvedené v Charte OSN patrí zriadenie mierových operácií, zavedenie medzinárodných sankcií a povolenie vojenských akcií. Svoje právomoci vykonáva prostredníctvom rezolúcií Bezpečnostnej rady OSN.

UN SECURITY COUNCIL RESOLUTION 1373 (2001)

Rezolúcia prijatá v roku 2001 vyžaduje od členských štátov, aby prijali sériu opatrení na boj proti terorizmu prostredníctvom prijatia zákonov a predpisov a vytvorenia administratívnych štruktúr. Rezolúcia tiež vyžaduje, aby si členské štáty „navzájom poskytovali čo najväčšiu pomoc pri vyšetrovaní trestných činov alebo trestných konaniach týkajúcich sa financovania alebo podpory teroristických činov“.

UNIQUE TRANSACTION REFERENCE NUMBER

Vzťahuje sa na kombináciu písmen, číslic alebo symbolov, ktorú určí poskytovateľ platobných služieb v súlade s protokolmi platobného a zúčtovacieho systému alebo systému zasielania správ, ktorý sa používa na prevod (pojem sa používa vo výkladovej poznámke k odporúčaniu FATF 16).

UNUSUAL TRANSACTION

Transakcia, ktorá sa zdá byť určená na obchádzanie požiadaviek na vykazovanie, nie je v súlade s transakčnými vzormi účtu alebo sa odchyľuje od činnosti očakávanej pre daný typ účtu.

USA PATRIOT ACT

Zákon o zjednotení a posilnení Ameriky poskytnutím vhodných nástrojov potrebných na zachytenie a zabránenie terorizmu z roku 2001 (Public Law 107-56). Tento historický zákon USA, ktorý bol prijatý 26. októbra 2001, priniesol významné zmeny v oblasti boja proti praniu špinavých peňazí vrátane viac ako 50 zmien a doplnení zákona o bankovom tajomstve. Hlava III zákona, International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, obsahuje väčšinu, ale nie všetky ustanovenia týkajúce sa boja proti praniu špinavých peňazí.

U-TURN PAYMENT

Platba, pri ktorej banka alebo iná inštitúcia z krajiny A odošle transakciu prostredníctvom banky v krajine B s využitím zahraničnej banky. Vo finančnom svete sú platby typu U-turn najčastejšie známe v súvislosti so sankciami USA - najmä so sankciami uvalenými na Irán.

VIENNA CONVENTION

Dohovor proti nezákonnému obchodu s omamnými a psychotropnými látkami z roku 1988. Krajiny, ktoré sa stanú zmluvnými stranami Viedenského dohovoru, sa zaväzujú kriminalizovať obchodovanie s drogami a s ním spojené pranie špinavých peňazí a prijať opatrenia na konfiškáciu príjmov z obchodovania s drogami. Článok III dohovoru obsahuje komplexnú definíciu prania špinavých peňazí, ktorá sa stala základom mnohých následných vnútroštátnych právnych predpisov.

VIRTUAL ASSET

Virtuálne aktívum je digitálna reprezentácia hodnoty, s ktorou možno digitálne obchodovať alebo ju previesť a ktorá sa môže použiť na platobné alebo investičné účely. Virtuálne aktíva nezahŕňajú digitálne reprezentácie fiat mien, cenných papierov a iných finančných aktív, ktoré sú už zahrnuté v iných častiach odporúčaní FATF. FATF aktualizoval usmernenie pre virtuálne aktíva v roku 2021 (vrátane DeFi a NFT). V júni 2023 vstúpilo do platnosti nariadenie EÚ MiCA (Market in Crypto-Assets Regulation) – plne aplikovateľné od decembra 2024 pre poskytovateľov krypto-aktív v EÚ.

VIRTUAL ASSET SERVICE PROVIDERS (VASP/CASP)

Poskytovateľom služieb virtuálnych aktív sa rozumie každá fyzická alebo právnická osoba, na ktorú sa nevzťahujú iné odporúčania a ktorá ako podnik vykonáva jednu alebo viacero z týchto činností alebo operácií pre inú fyzickú alebo právnickú osobu alebo v jej mene:

i. výmenu medzi virtuálnymi aktívami a fiat menami;

ii. výmenu medzi jednou alebo viacerými formami virtuálnych aktív;

iii. prevod virtuálnych aktív;

iv. úschova a/alebo správa virtuálnych aktív alebo nástrojov umožňujúcich kontrolu nad virtuálnymi aktívami a

v. účasť na finančných službách a poskytovanie finančných služieb súvisiacich s ponukou a/alebo predajom virtuálneho aktíva zo strany emitenta.

V tomto kontexte virtuálnych aktív znamená prevod uskutočnenie transakcie v mene inej fyzickej alebo právnickej osoby, ktorou sa virtuálne aktívum presúva z jednej adresy alebo účtu virtuálnych aktív na iný účet.

FATF aktualizované usmernenie pre VASP (2021): FATF vydal aktualizované usmernenie pre prístup k virtuálnym aktívam a poskytovateľom služieb virtuálnych aktív na základe rizika. Usmernenie spresňuje, že niektoré produkty decentralizovaných financií (DeFi) a nenahraditeľné tokeny

(NTF) môžu tiež spadať do rozsahu AML/CFT požiadaviek v závisloti od ich povahy a funkcie. Decentralizované platformy, ktoré v praxi vykonávajú funkcie VASP, by mali byť regulované rovnako ako VASP.

Nariadenie EÚ MiCA (Market in Crypto-Assets Regulation EÚ 2023/1144): vstúpilo do účinnosti v júni 2023 a plne sa vzťahuje na poskytovateľov krypto-aktív v EÚ (CASP – Crypto-Asset Service Providers) od decembra 2024. CASP sú povinní získať licenciu od príslušného orgánu dohľadu a spĺňať požiadavky AML/CFT. MiCA nahrádza roztrieštený národný rámec a zavádza jednotný európsky pas pre CASP v celej EÚ.

Travel Rule pre VASP/CASP: Podľa FATF Odporúčania č. 16 sú VASP povinní pri prevodoch virtuálnych aktív odovzdávať informácie o iniciátorovi a príjemcovi transakcie spolu s prevodom (tzn. Travel Rule). V rámci EÚ je Travel Rule pre krypto-aktíva záväzné od 30. decembra 2024 na základe nariadenia o prevode finančných prostriedkov (TFR, nariadenie EÚ 2023/1113). Táto povinnosť sa vzťahuje na prevody virtuálnych aktív bez ohľadu na výšku sumy transakcie.

VIRTUAL CURRENCY

Prostriedok výmeny, ktorý funguje v digitálnom priestore a ktorý sa zvyčajne dá konvertovať buď na fiat (napr. štátom emitovanú menu), alebo môže byť náhradou za reálnu menu.

WEAK ALIAS

Alternatívne meno alebo označenie sankcionovanej osoby či subjektu, ktoré je natoľko všeobecné alebo bežné, že jeho použitie pri sankčnom screeningu generuje neúmerne vysoký počet falošne pozitívnych zhôd. OFAC označuje takéto aliasy vo svojich sankčných zoznamoch ako „weak AKA“ práve s cieľom upozorniť používateľov na ich obmedzenú diskriminačnú hodnotu.

V kontexte AML/CFT a sankčného screeningu má správne zaobchádzanie so slabými aliasmi priamy dopad na efektívnosť screeningového procesu – použitie slabého aliasu ako primárneho vyhľadávacieho kritéria by zaplavilo compliance tímy obrovským množstvom irelevantných alertov vyžadujúcich manuálne preverenie, čím by sa výrazne znížila celková účinnosť sankčného programu. Finančné inštitúcie sú preto povinné pri konfigurácii svojich screeningových systémov zohľadniť označenie weak AKA v sankčných zoznamoch OFAC a nastaviť parametre tak, aby slabé aliasy neviedli k automatickému blokovaní transakcií bez ďalšieho kontextuálneho posúdenia – napríklad vyžadovaním zhody viacerých identifikačných atribútov súčasne ako mena, dátumu narodenia, národnosti alebo adresy pred vygenerovaním alertu. Správna kalibrácia zaobchádzania so slabými aliasmi je pritom jedným z aspektov posudzovaných regulátormi pri hodnotení primeranosti sankčného screeningového programu – príliš agresívne nastavenie vedie k operačnej neefektívnosti, zatiaľ čo ignorovanie slabých aliasov bez akéhokoľvek kontextuálneho skórovania môže viesť k prehliadnutiu skutočných zhôd.

WHITELIST

Zoznam osôb a subjektov, ktorých charakteristiky vyvolali pozitívnu lustráciu alebo upozornenie pomocou AST (automatického skríningového nástroja), ale ktoré sa nezhodujú so zoznamom sankcií. Niektoré AST umožňujú používateľom pripojiť doplňujúce informácie, ktoré podporujú záver, že táto osoba alebo subjekt nie sú cieľom sankcií a oprávňujú ich zaradenie na biely zoznam.

WILLFUL BLINDNESS

Právna zásada, ktorá sa uplatňuje v prípadoch prania špinavých peňazí v USA a ktorú súdy definujú ako „úmyselné vyhýbanie sa poznaniu skutočností“ alebo „zámernú ľahostajnosť“. Súdy rozhodli, že úmyselná slepota je ekvivalentom skutočnej vedomosti o nelegálnom zdroji finančných prostriedkov alebo o zámeroch klienta v rámci transakcie prania špinavých peňazí.

WIRE TRANSFER

Elektronický prenos finančných prostriedkov medzi finančnými inštitúciami v ich mene alebo v mene ich klientov. Bankové prevody sú finančné nástroje, na ktoré sa vzťahujú regulačné požiadavky mnohých krajín v rámci boja proti praniu špinavých peňazí.

WITHOUT DELAY

Výraz bezodkladne znamená v ideálnom prípade v priebehu niekoľkých hodín od určenia Bezpečnostnou radou OSN alebo jej príslušným sankčným výborom (napr. výborom 1267, výborom 1988, sankčným výborom 1718). Na účely S/RES/1373(2001) fráza bezodkladne znamená po tom, ako sa objavia primerané dôvody alebo rozumný základ na podozrenie alebo presvedčenie, že osoba alebo subjekt je teroristom, financuje terorizmus alebo je teroristickou organizáciou. V oboch prípadoch by sa slovné spojenie bezodkladne malo vykladať v kontexte potreby zabrániť úniku alebo rozptýleniu finančných prostriedkov alebo iných aktív, ktoré sú spojené s teroristami, teroristickými organizáciami, tými, ktorí financujú terorizmus, a s financovaním šírenia zbraní hromadného ničenia, a potreby globálnych, zosúladených opatrení na rýchle zadržanie a narušenie ich toku.

WOLFSBERG GROUP

Skupina Wolfsberg, pomenovaná podľa zámku vo Švajčiarsku, kde sa konalo jej prvé pracovné zasadnutie, je združením globálnych finančných inštitúcií vrátane Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank a UBS. V roku 2000 tieto inštitúcie spolu s Transparency International a odborníkmi z celého sveta vypracovali globálne usmernenia proti praniu špinavých peňazí pre medzinárodné súkromné banky. Odvtedy vydala okrem iného niekoľko ďalších usmernení týkajúcich sa korešpondenčného bankovníctva a financovania terorizmu. V marci 2023 Credit Suisse prevzala UBS v rámci záchrannej fúzie a teda Credit Suisse bola zo zoznamu vyradená.

WORLD BANK (WB)

Svetová banka je dôležitým zdrojom finančnej a technickej pomoci pre rozvojové krajiny. Nie je to banka v bežnom zmysle slova, ale tvoria ju dve jedinečné rozvojové inštitúcie, ktoré vlastní 184 členských krajín - Medzinárodná banka pre obnovu a rozvoj (IBRD) a Medzinárodné združenie pre rozvoj (IDA). Obe organizácie poskytujú rozvojovým krajinám pôžičky s nízkym úrokom, bezúročné úvery a granty. V roku 2002 MMF a Svetová banka spustili 12-mesačný pilotný program na hodnotenie opatrení krajín proti praniu špinavých peňazí a financovaniu terorizmu. Svetová banka a MMF v spolupráci s FATF vypracovali spoločnú metodiku na vykonávanie takýchto hodnotení na základe 40 odporúčaní FATF.

WGEL

Pracovná skupina EAG pre vzájomné hodnotenia a právne otázky.

WGTA

Pracovná skupina EAG pre technickú pomoc.

WGTYP

Pracovná skupina EAG pre typológie a boj proti financovaniu terorizmu a trestnej činnosti.

ZOZNAM ZDROJOV PRE OBLASŤ AML/CFT

I. FATF – Finančná akčná skupina (Financial Action Task Force)

- 40 odporúčaní FATF (aktualizované znenie 2023)
- Metodológia hodnotenia súladu s odporúčaniami FATF
- Usmernenia k prístupu založenému na riziku (Risk-Based Approach Guidelines)
- Usmernenia k virtuálnym aktívam a poskytovateľom služieb virtuálnych aktív (VASP, 2019, 2021, 2023)
- Usmernenia k financovaniu terorizmu (Terrorist Financing)
- Správa o financovaní proliferácie (Proliferation Financing, 2020)
- Správa o Trade-Based Money Laundering (TBML)
- Usmernenia k digitálnej identite (Digital Identity)
- Usmernenia k politicky exponovaným osobám (PEP)
- Usmernenia k skutočnému vlastníctvu (Beneficial Ownership)
- Usmernenia k de-riskingu (2021, 2023)
- Správy o vzájomnom hodnotení krajín (Mutual Evaluation Reports)
- Blacklist a Greylist FATF (aktualizované zoznamy jurisdikcií)
- Typológie a správy o nových rizikách (Emerging Risks Reports)
- Usmernenia k RegTech (2021)
- Správa FATF o NFT a DeFi

II. Regionálne orgány typu FATF (FATF-Style Regional Bodies – FSRBs)

- Moneyval – Výbor Rady Európy pre hodnotenie opatrení proti praniu peňazí
- MENAFATF – Blízky východ a severná Afrika
- APG – Ázijsko-tichomorská skupina
- GIABA – Medzivládna akčná skupina pre Afriku
- GAFILAT – Skupina pre finančné akcie v Latinskej Amerike
- ESAAMLG – Východná a južná Afrika
- GABAC – Stredná Afrika
- EAG – Eurázia

III. Legislatíva Európskej únie

- Smernica 2005/60/ES – 3. smernica AML (3AMLD)
- Smernica 2015/849/EÚ – 4. smernica AML (4AMLD)
- Smernica (EÚ) 2018/843 – 5. smernica AML (5AMLD)
- Smernica (EÚ) 2018/1673 – 6. smernica AML (6AMLD)
- Nariadenie (EÚ) 2024/1620 – Nariadenie o AMLA
- Nariadenie (EÚ) 2024/1624 – Nariadenie o predchádzaní praniu špinavých peňazí
- Nariadenie (EÚ) 2023/1113 – Nariadenie o transfere fondov (Travel Rule)
- Nariadenie (EÚ) 2023/1114 – MiCA (Markets in Crypto-Assets)
- Nariadenie (EÚ) 2015/847 – Nariadenie o informáciách sprevádzajúcich prevody peňažných prostriedkov
- Nariadenie (EÚ) 2016/679 – GDPR (ochrana osobných údajov, relevantné pre KYC)
- Smernica (EÚ) 2019/1153 – Smernica o využívaní finančných informácií
- Spoločný zoznam vojenského materiálu EÚ (EU Common Military List)
- Nariadenia EÚ o sankciách (geografické a tematické – Rusko, Irán, Severná Kórea, atď.)

IV. Medzinárodné dohovory a rezolúcie OSN

- Viedenský dohovor (1988) – Dohovor OSN proti nedovolenému obchodu s omamnými látkami
- Palermský dohovor (2000) – Dohovor OSN proti nadnárodnému organizovanému zločinu
- UNCAC (2003) – Dohovor OSN proti korupcii
- Merida dohovor – UNCAC implementačné usmernenia
- Rezolúcia BR OSN č. 1267 (1999) a nadväzujúce – sankcie voči Al-Káide a ISIS
- Rezolúcia BR OSN č. 1373 (2001) – financovanie terorizmu
- Rezolúcia BR OSN č. 1540 (2004) – nešírenie zbraní hromadného ničenia
- Rezolúcia BR OSN č. 2462 (2019) – financovanie terorizmu
- Sankčné zoznamy Bezpečnostnej rady OSN (Consolidated Sanctions List)

V. Regulačné orgány a ich usmernenia – Európa

- EBA (Európsky orgán pre bankovníctvo) – Usmernenia k riadeniu rizík ML/TF, k CDD, k outsourcingu
- EBA – Správa o de-riskingu
- EBA – Usmernenia k faktorom rizika (Risk Factor Guidelines, 2021)
- ESMA (Európsky orgán pre cenné papiere a trhy) – usmernenia k AML pre investičné firmy
- EIOPA (Európsky orgán pre poisťovníctvo) – usmernenia k AML pre poisťovne

- ECB (Európska centrálna banka) – usmernenia k AML dohľadu
- EuroFIU / FIU.net – spolupráca finančných spravodajských jednotiek EÚ

VI. Regulačné orgány a ich usmernenia – USA

- FinCEN (Financial Crimes Enforcement Network) – pravidlá BSA, usmernenia, SAR reportovanie
- OFAC (Office of Foreign Assets Control) – sankčné zoznamy SDN a programy
- OCC (Office of the Comptroller of the Currency) – BSA/AML usmernenia pre banky
- Federal Reserve – SR Letters k AML
- FDIC – Compliance examination procedures
- SEC – AML usmernenia pre broker-dealerów
- FINRA – AML pravidlá a usmernenia pre obchodníkov s cennými papiermi
- FinCEN – CDD Rule (Customer Due Diligence Requirements, 2016)
- US Bank Secrecy Act (BSA) – základ amerického AML rámca
- US PATRIOT Act (2001) – rozšírenie BSA po 9/11
- Anti-Money Laundering Act of 2020 (AMLA 2020, súčasť NDAA)
- Corporate Transparency Act (CTA, 2021) – skutočné vlastníctvo v USA
- Global Magnitsky Act (2016) a Executive Order 13818

VII. Regulačné orgány a ich usmernenia – Spojené kráľovstvo

- JMLSG (Joint Money Laundering Steering Group) – Guidance for the UK Financial Sector
- FCA (Financial Conduct Authority) – usmernenia k AML, Financial Crime Guide
- OFSI (Office of Financial Sanctions Implementation) – sankčné usmernenia
- NCA (National Crime Agency) – suspicious activity reports, typológie
- Proceeds of Crime Act 2002 (POCA) – hlavný britský AML zákon
- Terrorism Act 2000 a Counter-Terrorism Act 2008
- Economic Crime (Transparency and Enforcement) Act 2022

VIII. Medzinárodné inštitúcie a štandardizačné orgány

- FSB (Financial Stability Board) – správy o FinTech, kryptomenách a finančnej stabilite
- Bazilejský výbor pre bankový dohľad (BCBS) – Sound Management of Risks (2014, 2017)
- Egmont Group – štandardy a princípy pre finančné spravodajské jednotky (FIU)
- Wolfsberg Group – Wolfsberg AML Principles (korešpondenčné bankovníctvo, PEP, súkromné bankovníctvo, TBML, FinTech)
- Wolfsberg Group – Sanctions Screening Guidance
- Transparency International – Corruption Perceptions Index, správy o korupcii
- Basel Institute on Governance – Basel AML Index
- IMF (Medzinárodný menový fond) – správy FSAP, technická pomoc v oblasti AML/CFT
- Svetová banka – správy o AML/CFT, Asset Recovery (StAR initiative)

IX. Exportná kontrola a proliferácia

- Wassenaarovo dojednanie – Kontrolné zoznamy (zbrane, dual-use technológie)
- Austrálska skupina (Australia Group) – kontrola chemických a biologických materiálov
- NSG (Nuclear Suppliers Group) – kontrola jadrových materiálov
- MTCR (Missile Technology Control Regime) – raketové technológie
- US ITAR (International Traffic in Arms Regulations)
- US EAR (Export Administration Regulations) + Entity List, Denied Persons List
- EU Nariadenie o tovare s dvojakým použitím (Dual-Use Regulation 2021/821)

X. Profesijné asociácie a certifikácie

- ACAMS (Association of Certified Anti-Money Laundering Specialists) – štandardy, usmernenia, CAMS certifikácia
- ICA (International Compliance Association) – FICA/CKYC certifikácie
- CFCS (Certified Financial Crime Specialist) – ACFCS
- ACFE (Association of Certified Fraud Examiners) – CFE certifikácia
- Chartered Institute for Securities & Investment (CISI) – compliance štandardy
- PRMIA / GARP – riadenie rizík vo finančných inštitúciách

XI. Kľúčové sankčné zoznamy a databázy

- OSN Consolidated Sanctions List
- OFAC SDN List (Specially Designated Nationals and Blocked Persons)
- OFAC Non-SDN Lists (FSE, SSI, MEU a ďalšie)
- EU Consolidated Financial Sanctions List

- OFSI UK Consolidated List
- Interpol Red Notices
- Komerčné databázy (World-Check / Refinitiv, Dow Jones Risk & Compliance, LexisNexis Bridger Insight, ComplyAdvantage, Accuity)

XII. Odporúčaná odborná literatúra a publikácie

- FATF Annual Reports
- MONEYVAL Annual Reports
- FinCEN SAR Statistics (USA)
- Europol – správy o organizovanej trestnej činnosti (SOCTA, IOCTA)
- Europol – správy o financovaní terorizmu
- Unodc – správy o praní špinavých peňazí a trestnej ekonomike
- Basel AML Index (každoročné hodnotenie krajín)
- IMF Global Financial Stability Reports (GFSR)
- Transparency International – správy a indexy

G. Lehnert
LAWYERS WITH INTEGRITY

G. Lehnert, s. r. o.
Budova ORBIS, Rajská 7, SK-811 08 Bratislava
lehnert@lehnert.sk | www.lehnert.sk