

prof. dr Stefan V. Milojević, PhD¹
prof. dr Snežana P. Knežević, PhD²
Aleksandra Mitrović³

PRANJE NOVCA U INDUSTRIJI OSIGURANJA

PREGLEDNI NAUČNI RAD

Apstrakt

Pranje novca predstavlja veoma komplikovanu aktivnost, koja ima za cilj da se izvor i prirodi prljavog novca prikrivaju kako bi novac izgledao zakonito, a zatim postao upotrebljiv i prenosiv, te stoga predstavlja ozbiljnu pretnju finansijskom sistemu. Pored osnovne svrhe kojoj je namenjeno, osiguranje se takođe može koristiti kao finansijski instrument za aktivnosti pranja novca. Pranje novca ili finansiranje terorizma su postale prilika za kriminalce da legalizuju svoj crni novac iz poslova koji se odnose na osiguranje. Cilj ovog istraživanja jeste da otkrije potencijalne indikatore koji mogu poslužiti kao mogućnosti za pranje novca i da se razmotre mogućnosti prevencije. Borba protiv pranja novca kao kriminalne aktivnosti u osiguravajućoj industriji je kontinuirani poduhvat koji zahteva fleksibilnost, jer su metode pranja novca promenljive i aktivnosti kojima se realizuje pranje novca, sve složenije. Rezultati ukazuju da je efikasna prevencija kao prva linija odbrane od pranja novca u osiguranju, moguća uz primenu regulatornog nadzora, savremenih tehnoloških rešenja i kontinuirane obuke zaposlenih o rizicima pranja novca i procedurama iz oblasti usklađenosti poslovanja (compliance). Zaključuje se da industrija osiguranja

¹ Associate Professor, Educons University, Faculty of Business Economics, Vojvode Putnika 87, 21208 Sremska Kamenica, Serbia, imejl: stefan.milojevic@educons.edu.rs. ORCID ID 0000-0001-6240-6776.

² Full Professor, University of Belgrade, Faculty of Organizational Sciences, Jove Ilića 154, 11010 Belgrade, imejl: snezana.knezevic@fon.bg.ac.rs ORCID ID 0000-0001-9833-7274.

³ Associate Professor, University of Kragujevac, Faculty of Hotel Management and Tourism in Vrnjačka Banja, imejl: aleksandra.stankovic@kg.ac.rs ORCID ID 0000-00028302-0853.

Rad primljen: 26.3.2026.

Rad prihvaćen: 11.6.2026.

i dalje predstavlja značajan kanal rizika koji zahteva stalno unapređenje sistema kontrole i nadzora.

Ključne reči: osiguranje, rizik, pranje novca, usklađenost poslovanja.

JEL classification: G22, K42, G18.

I UVOD

Pranje novca (money laundering – ML; ili „blanqueo“ na španskom, „blanchiment“ na francuskom, „riciclaggio“ na italijanskom, i slični termini na drugim jezicima), se široko shvata kao proces prikrivanja kriminalnog porekla imovine i investicija ili nezakonite prirode finansijske transakcije).⁴ Predstavlja proces fabrikovanja velike količine kapitala stečenog bilo kakvim nezakonitim ili neetičkim radnjama koje se sastoje od ozbiljnih krivičnih dela kao što su trgovina drogom, mafija, terorizam itd.⁵ Prema drugoj definiciji, pranje novca može se definisati kao tehnika koju kriminalci koriste za prikrivanje porekla nezakonitih prihoda sa namerom da uživaju u svom „očišćenom“ novcu, bez uplitanja rivala iz podzemlja ili primene zakona.⁶

Pranje novca je, na šta je ukazano, može biti definisano na različite načine iz različitih izvora. Iako su definicije koje koriste razni regulatorni organi, krivični zakoni i agencije za sprovođenje zakona validne, svi izvori se fokusiraju na svoje polje delovanja (krivične aspekte, računovodstvene aspekte ili na nezakonitu prirodu akcija).

Pranje novca na internetu toliko je komplikovano da je teško odlučiti gde se ono tačno događa. Takođe je prilično teško utvrditi i koji organ je nadležan za istragu i krivično gonjenje transnacionalnog kriminalnog akta.⁷

Kriminalci zapravo realizuju aktivnosti pranja novca u svrhu osujećivanja istrage i onemogućavanja krivičnog gonjenja. Tačna definicija pranja novca varira u zavisnosti od jurisdikcija. Pranje novca pretvara ilegalni novac (ilegalna sredstva) u imovinu koja deluje legitimno. Pranje novca se može sagledati kao složen proces, raščlanjen na tri elementa: plasman, slojevitost i integracija nezakonitih

⁴ Ernesto Ugo Savona, Michale De Feo, "International money laundering trends and prevention/control policies.", *Responding to Money Laundering: International Perspectives* (ed. E. Savona), Harwood Academic, Amsterdam, 1997, 9–71.

⁵ Ayush Kumar et al., "Fraud Detection in Anti-money Laundering System Using Machine Learning Techniques", *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences. Algorithms for Intelligent Systems* (ed. Mayank Dave et al.) Springer, Singapore, 2020.

⁶ Jeffrey Simser, "Money Laundering: Emerging Threats and Trends.", *Journal of Money Laundering Control*, No. 1/2012, 41–54.

⁷ Ping He, "A typological study on money laundering", *Journal of Money Laundering Control*, No. 1/2010, 15–32.

prihoda (Slika 1). Iako je drevni fenomen, prvi put je proglašeno ilegalnim tek 1986. godine.⁸

Slika 1. Osnovni koraci u procesu pranja novca

Plasman	Raslojavanje	Integracija
Novac je deponovan u banci	Fondovi su preneseni u inostranstvo, uglavnom u kompanije “školjke” ili je prerušen u prihode legitimnih firmi.	Lažna otpлата zajma ili falsifikovani računi koji se koriste kao pokriće za oprani novac
Novac je fizički prenesen u inostranstvo	Depoziti su napravljeni u inostranim bankarskim sistemima ili u bliskim bankama.	Kompleksna mreža transfera (kako domaćih tako i međunarodnih) čini izvor sredstava praktično nemogućim za otkrivanje
Novac je upotrebljen za kupovinu robe visoke vrednosti, nekretnina ili firmi.	Prethodno kupljena roba i nekretnine su prodane za novac.	Prihod od nekretnina ili legitimnih poslovanja ima izgled legitimnosti

Izvor: Elizabeth Vallery Mulig, Murphy Smith, “Understanding and preventing money laundering”, *Internal auditing*, No. 5/2008, 22–25

Često se povezuje sa narkoticima, korupcijom, prostitucijom, ilegalnom trgovinom oružjem, utajom poreza i finansiranjem terorizma. Proces identifikovanja ovih vrsta aktivnosti pranja novca naziva se sprečavanje pranja novca (*Anti-Money Laundering - AML*). Ova imovina može izgledati kao polise osiguranja, bankovni depoziti, kao i nekretnine. Aktivnosti pranja novca nisu ograničene samo na finansijske institucije, jer se nefinansijske institucije, kao što su turističke agencije, industrija nekretnina, kazina i kockanje, sada koriste za pranje novca. Priroda pranja novca, međutim, u industriji osiguranja razlikuje se od prirode u drugim industrijama. Sektor osiguranja je uglavnom strukturisan iz osiguravajućih društava, agencija za osiguranje, brokera i reosiguravača. Specifičnost poslovanja osiguravajućih društava je ovičena fundamentalnom prirodom njihovog poslovanja, kao i rizika koji su im srodni.⁹

Da bi napori protiv pranja novca bili efikasni, mora postojati okruženje pogodno za pošteno i otvoreno izveštavanje. Pravni autoriteti, političari i javnost

⁸ Jason Sharman, “Power and discourse in policy diffusion: anti-Money laundering in developing states”, *International Studies Quarterly*, No. 3/2008, 635-656

⁹ Snežana Knežević, „Faktori kvaliteta finansijskog izveštavanja osiguravajućih društava“, Referat na XLII Simpozijumu Saveza računovođa i revizora Srbije, Zlatibor, 2011, 411–427.

moraju imati podršku. Međunarodna federacija računovođa (*International Federation of Accountants – IFAC*), u nastojanju da stvori takvo okruženje, podstiče svoje organe da uspostavljaju kolaborativne odnose sa zakonodavnim i regulatornim vlastima, kako korporativnim, tako i političkim.

Pranje novca na globalnom nivou nameće značajne troškove svetskoj ekonomiji time što nanosi štetu efikasnom poslovanju nacionalnih ekonomija i promovisanjem lošije ekonomske politike. Kao rezultat toga, finansijska tržišta polako postaju korumpirana, a poverenje javnosti u međunarodni finansijski sistem biva narušeno, tako da sve skupa ima negativne posledice po rast svetske privrede. Zbog svega ovoga, zabrinutost zbog pranja novca stiže iz mnogih pravaca.¹⁰

Pranje novca predstavlja sistemski rizik za finansijsku i ekonomsku sferu, kao i za nacionalnu bezbednost svih zemalja.¹¹ Brojne domaće i međunarodne grupe bave se pranjem novca. SAD imaju rigorozne zakone protiv pranja novca i oni uključuju:

- Zakon o suzbijanju zloupotrebe droga iz 1988. godine,
- Zakon o kontroli kriminala iz 1990. godine,
- Zakon Annuzio-Wylie iz 1992. godine,
- Zakon o suzbijanju pranja novca iz 1994. godine,
- Zakon o sprečavanju terorizma iz 1995. godine,
- Novi zahtevi finansijskim institucijama za izveštavanje iz 1996. godine, i
- *USA Patriot Act (USAPA)* iz 2001. godine.

Međunarodni naponi u borbi protiv pranja novca nalaze se u Svetskoj banci, Međunarodnom sporazumu i FATF (*Financial Action Task Force*). Svetska banka promoviše mere koje zaustavljaju ili usporavaju priliv novca na tržišta u usponu. Međunarodni sporazumi uključuju Bečku konvenciju, Konvenciju Saveta Evrope iz 1990. godine, Bazelski izveštaj principa, Direktivu Evropske unije i Rezoluciju Međunarodne organizacije komisija za hartije od vrednosti.¹²

Evolucija različitih propisa i amandmana koje su uveli regulatori bila je neminovnost u odnosu na to kako su osiguravači bili izloženi novijim načinima i mehanizmima razvoja alata i sredstava finansijskog kriminala. Ključnu ulogu u definisanju jedinstvenih međunarodnih standarda za SPN/FT ima Radna grupa za finansijsku akciju (FATF). FATF razvija i postavlja međunarodne standarde SPN/FT, neguje neophodnu političku volju za sprovođenje regionalnih i nacionalnih regulatornih reformi i procenjuje efikasnost mera koje primenjuju pojedinačne zemlje.

Kada je reč o Srbiji, primarni zakon o SPN/FT je Zakon o sprečavanju pranja novca i finansiranja terorizma (Zakon o SPNiFT¹³). Ovim zakonom su propisane radnje

¹⁰ Helsingin Sanomat, *Criminals Rush for Euros*, Helsinki, Finland, 2001.

¹¹ Oleg Reznik, Maryna Utkina, Olha Bondarenko, „Financial intelligence (monitoring) as an effective way in the field of combating money laundering”, *Journal of Money Laundering Control*, No. 1/2023, 94-105.

¹² Elizabeth Vallery Mulig, Murphy Smith, „Understanding and preventing money laundering”, *Internal auditing*, No. 5/2008, 22–25.

¹³ Zakon o sprečavanju pranja novca i finansiranja terorizma, *Sl. glasnik RS*, br. 113/2017, 91/2019, 153/2020, 92/2023, 94/2024 i 19/2025.

i mere koje se preduzimaju radi sprečavanja i otkrivanja pranja novca i finansiranja terorizma. Pored toga, njime se reguliše nadležnost Uprave za sprečavanje pranja novca i nadležnost drugih organa za sprovođenje odredaba Zakona o SPNiFT, što uključuje i nadzor nad primenom njegovih odredbi. Prema članu 4, obveznici ovog zakona jesu: društva za osiguranje koja poseduju dozvolu za obavljanje životnih osiguranja i društva za posredovanje u osiguranju kada obavljaju poslove posredovanja u životnim osiguranjima; društva za zastupanje u osiguranju i zastupnici u osiguranju, koji imaju dozvolu za obavljanje poslova osiguranja života, osim društava za zastupanje i zastupnika u osiguranju za čiji rad odgovara društvo za osiguranje u skladu sa zakonom.

FATF ukazuje na nekoliko upozoravajućih znakova koji mogu upozoriti kompanije na potencijalno pranje novca, deleći ih u sledeće kategorije:

Tabela 1. *Red flags* (indikatori upozorenja na potencijalno pranje novca)

Kategorija indikatora upozorenja	Primer
Ponašanje klijenta	Klijent je preterano tajanstven ili izbegava da pruži informacije o svom identitetu.
Poreklo sredstava	Klijent koristi više bankovnih računa bez opravdanog poslovnog razloga.
Nepotrebno korišćenje pravnih stručnjaka ili složenih pravnih struktura	Klijent angažuje advokatsku kancelariju radi osnivanja više ošor kompanija i trustova u različitim jurisdikcijama.
Priroda angažmana	Klijent učestvuje u transakcijama koje nisu u skladu sa njegovim uobičajenim poslovnim aktivnostima.
Geografski rizik	Klijent potiče iz jurisdikcije ili posluje sa jurisdikcijom poznatom po visokom nivou korupcije, slaboj primeni propisa za sprečavanje pranja novca ili međunarodnim sankcijama.

Izvor: preuređeno prema FATF Guidance.

Sumnjiva transakcija je svaka nameravana ili izvršena transakcija u vezi sa kojom zaposleni zna ili ima osnova da posumnja da imovina ili sredstva potiču od predikatnog krivičnog dela za pranje novca ili su povezana sa finansiranjem terorizma. Trgovina drogom je glavni predikatno krivično delo za pranje novca, a rizik od pranja novca varira u zavisnosti od nivoa aktivnosti u vezi sa drogom.¹⁴

Svaki zaposleni banke, bez obzira na poziciju, ukoliko otkrije osnove sumnje u pranje novca ili finansiranje terorizma, bez odlaganja treba da o tome informiše lokalno ovlašeno lice za sprečavanje pranja novca, a koje je u obavezi da obezbedi svu profesionalnu pomoć u proceni sumnje.

¹⁴ J. Simser, "Money laundering: emerging threats and trends". *Journal of Money Laundering Control*, No. 1/2012, 41–54.

Postoji veliki broj opštih indikatora upozorenja, a u nastavku su predstavljeni još neki o njih:

- klijent se detaljno raspituje kod stručnih lica za načine kojima može izbeći prijavljivanje transakcija FOS-u,
- klijent pokazuje znakove uplašenosti,
- klijent ima neuobičajeno dobro znanje o propisima i zahtevima iz oblasti sprečavanja pranja novca i finansiranja terorizma,
- pravo raspolaganja sredstvima na istom računu imaju osobe (više osoba) za koje je jasno da nisu u sredstvu sa vlasnikom računa,
- poslovni odnos je uspostavljen sa pravnim licem za koje je poznato da ima isto poslovno sedište i istog zakonskog zastupnika kao neko drugo pravno lice,
- nemoguće je uočiti logičku vezu između izvršenih transakcija i poslovnih aktivnosti klijenta,
- klijent vrši (gotovinske i bezgotovinske) transakcije u iznosima koji su neznatno ispod limita za prijavu transakcija FOS-u,
- klijent polaže neuobičajene iznose gotovog novca, a to nije u srazmeri sa njegovim uobičajenim obimom poslovanja,
- klijent koristi poslovni račun što nije u skladu sa svrhom za koju je račun otvoren,
- klijent nesporedno nakon (ili neposredno pre) realizacije transakciju koja se tiče gotovine - pristupa sefu,
- poslovni odnos je uspostavilo fizičko ili pravno lice koje bi moglo biti dovedeno u vezu sa nekom terorističkom organizacijom.

Posebno je važno istaći značaj usklađivanja sajber prostora i elektronske uprave u srodnim organizacijama, uključujući banke, berze, osiguravajuća društva, nacionalnu organizaciju za civilnu registraciju, nacionalnu organizaciju za registraciju dokumenata i nekretnina, nacionalnu organizaciju za registraciju preduzeća i komercijalnih preduzeća, kako bi se na najbolji način dao doprinos u borbi protiv pranja elektronskog novca. Vladini zvaničnici bi trebalo snažno da razmotre pripremu ažuriranih zakona i propisa, infrastrukturu, kulturu, javno prihvatanje i međunarodnu saradnju.¹⁵ Sve veća integracija globalnih finansijskih sistema i uklanjanje barijera postavljenih ispred slobodnog kretanja kapitala stvaraju povoljne uslove za kriminalne strukture za pranje novca, odnosno olakšavaju pranje crnog novca i uslo-žnjavaju praćenje novca. Poznata je činjenica da se u kontinuitetu, lažne odštete (koje se ne mogu dovesti u vezu sa novcem), bile jedan od poznatijih aspekata industrije osiguranja. Imajući u vidu da je sve veći obim novčanih transakcija iz dana u dan, već duže vreme, sektor osiguranja koriste i perači novca za pranje prihoda od kriminala.

¹⁵ Ghorban Daniali, "E-money laundering prevention", *New Marketing Research Journal*, Special Issue, 2014, 29–38.

Ostatak rada je strukturiran na sledeći način: Odeljak 2 ukazuje na prevare i fenomen pranja novca. Odeljak 3 bavi se specifičnostima industrije osiguranja po pitanju pranja novca. Odeljak 4 ukazuje na kritične tačke u industriji osiguranja i daje odgovarajuće preporuke, dok odeljak 5 zaključuje rad.

II PREVARE U OSIGURANJU I FENOMEN PRANJA NOVCA

Prema *Black's Law Dictionary*,¹⁶ prevara je „svesno pogrešno predstavljanje istine ili prikrivanje materijalne činjenice kako bi se drugog navelo da deluje na svoju štetu“. Četiri glavna elementa prevare su: (1) lažna izjava o (2) materijalnoj činjenici koja je (3) namerno učinjena sa (4) namerom da se obmane. Prevare su danas rasprostranjene u svim segmentima industrije: bankarstvu i finansijskim uslugama, osiguranju, telekomunikacijama, maloprodaji, transportu i vladinim organizacijama, a razlikuju se po intenzitetu i složenosti.¹⁷ Prevare u osiguranju su značajan izazov za osiguravajuća društva, jer dovode do finansijskih gubitaka, destabilizacije tržišta i gubitka poverenja klijenata. Kako bi se zaštitila osiguravajuća društva pojedinačno, s jedne strane, i obezbedila održivost industrije osiguranja, s druge strane, neophodno je efikasno upravljanje rizikom od prevara.¹⁸

Za krivično delo pranja novca mora postojati predikatno krivično delo. Ne možemo razmatrati pranje novca bez tzv. predikatnog krivičnog dela (osnovnog krivičnog dela kojim se generiše tzv. oprana imovina). Upravo u tom kontekstu, 6. SPN Direktiva (6AMLD)¹⁹ daje usklađenu listu predikatnih krivičnih dela koja, pored standardnih krivičnih dela u vezi sa pranjem novca, kao što su trgovina drogom, ljudima, nedozvoljena trgovina oružjem, korupcija i prevara, a takođe obuhvata i poreska dela, ekološki kriminal i sajber kriminal. Prevare je veoma čest predikatno krivično delo koje dovodi do pranja novca. Pošto finansijske institucije imaju jedinice za prevare i jedinice za sprečavanje pranja novca, logično je da te dve jedinice rade zajedno i u skladu jedna sa drugom.²⁰ FRAML je termin koji se koristi za kombinaciju prevare i sprečavanja pranja novca (FRAUD + AML).

¹⁶ Bryan A. Garner, *Black's Law Dictionary*, Thomson West, Eagan, 2019.

¹⁷ Girish Keshav Palshikar, "Detecting Frauds and Money Laundering: A Tutorial", *Big Data Analytics* (eds. Srinath Srinivasa, Sameep Mehta), Springer, Cham, 2014.

¹⁸ Stefan Milojević, Snežana Knežević, Vladimir Šebek, „Upravljanje rizikom od prevara u osiguranju“, *Tokovi osiguranja*, br. 4/2024, 938-961.

¹⁹ Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. <https://eur-lex.europa.eu/eli/dir/2018/1673/oj/eng>, 3.3.2026.

²⁰ Kelvin Sullivan, "Fraud and Anti-Money Laundering. In: Anti-Money Laundering in a Nutshell", *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers* (ed. Kevin Sullivan), Apress, Berkeley, CA, 2023, 219-229.

Relevantna su dva pitanja: ko čini prevare i koje su vrste prevara prisutne u osiguranju. Izveštaj FBI-2²¹ navodi da industrija osiguranja u SAD, gubi oko 40 milijardi dolara godišnje na prevare samo u sektoru ne-zdravstvenog osiguranja. Kada su u pitanju počinioci prevara u osiguranju, uobičajeno se navode sledeći: nepošteni osiguranici, ljudi iz osiguravajuće industrije (tj. agenti, brokери, rukovodioci kompanija) i labavo organizovane mreže korumpiranih medicinskih stručnjaka i advokata koji koriste svoje znanje da zaobiđu mere protiv prevara koje su uvele osiguravajuće kompanije.²²

Razne vrste prevara su prisutne u osiguranju. Klijenti spremni da prihvate nepovoljnu polis, učešće neotkrivene strane, preuveličana potraživanja/lažna ili lažna potraživanja su uobičajene prevare u osiguranju. Potraživanja koja prate lažna smrt i gubitak pamćenja su česta prevara u životnom osiguranju. Neplaćanje premija, nesrazmerna provizija i polise osiguranja od nepostojećih kompanija. Nestručna medicinska dokumenta, polise sa zakašnjenjem, iznuda putem falsifikovanja, čak i otmica i ubistvo, su druge strategije kriminalaca kod poslova u osiguranju.

Prema "National Insurance Crime Bureau" (NICB) se kao opšti indikatori prevara u osiguranju kada je reč o gubitku u vezi sa zalihama mogu uključivati sledeće:²³

- Prevara sa gubitkom zaliha/imovinskom prevarom.
- Osiguranik je nedavno razdvojen ili razveden.
- Računi se podnose nedeljama ili mesecima nakon što je posao obavljen.
- Polisa se otkazuje ubrzo nakon podnošenja zahteva, često zbog neplaćanja premije.
- Gubici nisu kompatibilni sa zanimanjem i/ili prihodima osiguranika.
- Gubici uključuju velike iznose gotovine.
- Prevara sa gubitkom zaliha/požarom.
- Kućni ljubimci nisu bili prisutni u vreme požara.
- Gubici uključuju stare ili neprodajne zalihe ili ilegalne hemikalije i materijale.
- Osiguranik ili osiguranikovo preduzeće ima finansijske poteškoće (bankrot ili zaplenu).
- Istraga otkriva da nema ostataka nezapaljivih predmeta iz imovine (novčići, kolekcije oružja ili nakit).
- Požar se dogodio noću posle 23:00.
- Vatrogasna služba izveštava da je uzrok zapaljiv, sumnjiv ili nepoznat.
- Gubitak zaliha/provala i krađa.

²¹ <http://www.fbi.gov/stats-services/publications/insurance-fraud>, 2.2.2025.

²² Investigating Insurance Fraud: A \$30-Billion-a-Year Racket, <https://www.fbi.gov/news/stories/investigating-insurance-fraud>, 3.5.2026.

²³ Indicators of Property Fraud: Individuals & Professionals Involved/Circumstances & Documents Detection -The First Line of Defence, file:///C:/Users/Sdoku/OneDrive/Desktop/Property%20Fraud%20(1%20of%203)2021.pdf.

- Komercijalni gubici se javljaju na mestu gde je malo ili nimalo bezbednosnih mera.
- Proces gubitka zaliha/potraživanja.
- Izgubljene zalihe osiguranika se značajno razlikuju od izveštaja o krivičnom delu policijske uprave.
- Osiguranik dostavlja račun(e) bez logotipa prodavnice (prazan račun).
- Osiguranik dostavlja dva različita računa sa istim rukopisom ili fontom.
- Osiguranik dostavlja jedan račun sa različitim rukopisom ili fontom.

Pranje novca se često naziva „prljavom malom tajnom“ finansijskog sveta.²⁴ Smith²⁵ ističe da uobičajene šeme koje se koriste za pranje novca uključuju *shell* kompanije, ofšor račune, kockanje, kriptovalute, transakcije sa neobičnim karakteristikama, politički eksponirane osobe (*Politically Exposed Person - PEP*²⁶), geografski rizik, nejasno krajnje korisno vlasništvo i iznenadne promene u uputstvima. Globalni finansijski sistem je postao međusobno povezaniji. Javno „imenovanje i sramota“, primoralo je pored ostalog, i osiguravajuće kompanije da poboljšaju svoje komplajans sisteme i ulažu u nove tehnologije koje mogu da otkriju i potencijalno spreče pranje novca.²⁷ Promena sa reaktivnog na proaktivni način u upravljanju rizikom od pranja novca i finansiranja terorizma, postala je neminovnost u ovom veoma dinamičnom okruženju.

III PRANJE NOVCA U INDUSTRIJI OSIGURANJA

Sa opšteg stanovišta, „pranje novca je termin koji se koristi za opisivanje šeme u kojoj kriminalci pokušavaju da prikriju identitet, originalno vlasništvo i određite novca koji su stekli kriminalnim ponašanjem“.²⁸ Pranje novca često uključuje složeni niz transakcija i brojne finansijske institucije iz mnogih oblasti. Nebankarski finansijski elementi, kao što su razmene novca, usluge unovčavanja čekova, osiguravajuće kompanije, posrednici i trgovci, takođe se sve više koriste kao instrumenti pojedincima koji se bave pranjem novca.

²⁴ Sven Stumbauer, „Basics of Anti-Money Laundering Compliance“, *The Next Wave of Global Anti-Money Laundering Enforcement*, Palgrave Macmillan, Cham, 2024, 21-26.

²⁵ Dunan Smith, „Common Money Laundering Schemes and Red Flags or Warnings of It“, *Money Laundering, Terrorist Financing and Virtual Assets: Cases and Materials*, Springer, Cham 2024, 35-46.

²⁶ Politički eksponirana osoba (PEP) je osoba kojoj je poverena ili je poverena istaknuta funkcija. Mnogi među njima zauzimaju položaje koji se mogu zloupotребiti u svrhu pranja nezakonitih sredstava ili drugih prestupnih dela kao što su korupcija ili podmićivanje. FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22). <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html>, 12.3.2026.

²⁷ S. Stumbauer.

²⁸ M. Lijuan, „Anti-Money Laundering“, *Dictionary of Contemporary Chinese Economics* (ed. Hong Yinxing), Springer, Singapore, 2025.

Pranje novca putem osiguravajućih institucija služi za prikrivanje porekla i prirode nezakonitih prihoda, kao i dobiti stečenih kupovinom, izmenom i predajom polisa osiguranja i podnošenjem zahteva za osiguranje kako bi se sprečilo praćenje od strane nadležnih.²⁹ Osiguravajuće institucije u velikoj meri korišćene od strane perača novca, te je logično postaviti pitanje, zbog čega su one za njih privlačne. Razni su razlozi za to, ali uopšteno govoreći, karakteristike osiguravajuće delatnosti i relativno slabo mešanje pravnog sistema na ovom tržištu jesu ključne odrednice.

Načini pranja novca uključuju šverc gotovine, korišćenje banaka ili osiguravajućih društava, ili korišćenje *shell* kompanija ili *front* kompanija. Danas se kriminalci okreću i nekretninama, lutriji, međunarodnoj trgovini, ofšor kompanijama kako bi prali novac. Ponekad perači novca iskorišćavaju advokate i računovođe. Sa širokom upotrebom elektronskog novca i interneta, kriminalci više vole da peru novac putem transakcija licem u lice. Postavlja se i pitanje da li su se perači novca okrenuli od banaka ka osiguravačima.

Proizvodi osiguranja, posebno u životnom osiguranju, pružaju veoma atraktivan i jednostavan način pranja novca. Posebno su ranjivi proizvodi životnog osiguranja investicionog tipa. Acharya dodaje da, iako je sektor životnog osiguranja veoma ranjiv, podjednako postoji rizik od pranja novca i finansiranja terorizma kroz opšte osiguranje, reosiguranje, posrednike i agente.³⁰

Prema FinCEN-u, „najznačajniji rizici pranja novca i terorizma u osiguravajućoj industriji nalaze se u proizvodima životnog osiguranja i anuiteta, jer takvi proizvodi omogućavaju klijentu da uloži velike količine sredstava u finansijski sistem i da ih besprekorno prebaci kako bi prikrivao njihovo pravo poreklo“³¹

Transakcije koje bi trebalo da privlače pažnju AML eksperata, jesu:

- velike isplate premija u gotovini,
- neuobičajene strukture polisa,
- česte promene u određivanju korisnika, i
- geografski regioni visokog rizika.

U osiguranju je bitno poći od usvajanja pristupa zasnovanog na riziku. Od osiguravajućih kompanija se očekuje da procene rizike od pranja novca koji se dovode u vezu sa povezanim poslovnim operacijama i klijentima, kao i da primene mere srazmerne ovim rizicima. Na primer, klijenti ili transakcije visokog rizika mogu zahtevati stroži CDD (radnje i mere poznavanja i praćenja klijenta - *Customer due diligence*³²) i praćenje.

²⁹ P. He, "A typological study on money laundering". *Journal of Money Laundering Control*, No. 1/2010, 15–32.

³⁰ Acharya Suman, Money Laundering (ML) and Terrorism Financing (TF) in the Insurance Market: A Risk and Vulnerability, dostupno na: <https://ssrn.com/abstract=2604560> or <http://dx.doi.org/10.2139/ssrn.2604560>, 11. 6. 2026.

³¹ Financial Crimes Enforcement Network, dostupno na: <https://www.fincen.gov/>, 4.4.2026.

³² Postoje tri vrste mera: Pojednostavljenje radnje i mere - *Primenjuju se na niskorizične klijente*; Opšte radnje i mere - *Primenjuju se na srednerizične klijente*; Pojačane radnje i mere - *Primenjuju se na visokorizične klijente*.

Za uspešnu borbu protiv pranja novca važno je da svi učesnici u finansijskom sektoru dosledno primenjuju proveru klijenata (*Know Your Customer* - KYC) i praćenje i analizu klijenata (CDD).³³ KYC i AML su snažni dopunski elementi jedno drugom i važni elementi za osiguravajuća preduzeća koja žele da se zaštite od prevare i finansijskog kriminala. Oba uključuju proveru identiteta i legitimитета pojedinaca i organizacija kroz rigorozne provere. Samo po sebi, to otežava rad kriminalaca. Pored toga, AML provere pomažu u otkrivanju traga novca, razumevanju odakle novac dolazi i kako se troši, tako da organizacije mogu da osiguraju da se ne pere preko njih.³⁴

Osiguravači mogu biti ranjivi na rizik od AML u raznim segmentima.³⁵ Prvi slučaj (opšte osiguranje) je kada se kupuju predmeti visoke vrednosti gde je izvor prihod od kriminalnih aktivnosti, nakon čega se podnose lažni zahtevi radi nadokande gubitaka. Ovim se postiže da se nadoknade dobijene od strane osiguravača tretiraju kao čist izvor finansiranja. Drugi slučaj podrazumeva da kupuju polise jednokratne premije kako bi to obezbedilo priliku licima koja se bave kriminalom, što dalje povlači prebacivanje značajnih suma novca u ekosistem finansijskih usluga. Treći slučaj se odnosi na ugovore o anuitetu gde se po osnovu planova osiguranja isplaćuje redovan prihod u zamenu za jednokratnu isplatu u gotovini unapred. Ovom aktivnošću se pruža prilika da perači novca mogu da zamene deo prljavog novca za redovan tok legitimnih prihoda. Četvrti slučaj se odnosi na "Cooling-off" period. Ovde se radi o tome da finansijska regulativa zahteva od osiguravača da ponude povraćaj plaćenih premija ako osiguranik odluči da otkáže u određenom roku nakon kupovine osiguranja. Takvi povraćaji efikasno pružaju peraćima novca čist izvor finansiranja. Peti slučaj se odnosi na klazule o predaji. Naime, mnoge polise osiguranja, uključujući planove štednje, nude osiguranicima mogućnost prevremene predaje, iako je to obično uz finansijski trošak. Za perače novca, ove klauzule pružaju sredstvo za obezbeđivanje isplate legitimnih sredstava, čak i ako su započeli polis u prljavim novcem. Sledeće, kod šestog slučaja se radi o prodaji polisa. Naime, za mnoge polise osiguranja sada postoji prosperitetno – i sasvim legitimno – sekundarno tržište gde se pokriće može prodati, a to je dobra opcija za perače novca jer mogu, da prodaju svoju polis u paušalnu sumu koja dolazi iz legitimnih izvora.

Još jedan slučaj je poznat (sedmi po redu), gde je reč o polisi kredita. Poznato je da su neki osiguravači voljni da daju kredite uz vrednost planova životnog osiguranja značajne vrednosti, uz obavezu da se ovaj plan tretira kao kolateral tokom procesa kreditiranja. Za perače novca je ovo jednostavan put do jednokratne

³³ Mirko Nazzari, Peter Reuter, „How well does the money laundering control system work?“, *Crime and Justice*, No. 1/2025, 67-152.

³⁴ Zanimljivo je pomenuti praksu na Mauricijusu, gde su svaka banka i osiguravajuća kompanija morale da kontaktiraju svakog vlasnika bankovnog računa i polise i da ih zamole da se lično jave sa identifikacijom (uključujući i premijera, koji se žalio na neprijatnosti), a ukoliko se oni ne pojave, njihovi računi i polise dobijaju status "zamrznute". J. Sharman. 635-656.

³⁵ Where insurers may be vulnerable to AML risk, dostupno na: <https://kyc360.com/platform>, 2.2.2026.

gotovine iz legitimnog izvora. Njima u prilog ide i činjenica da su takvi krediti manje praćeni u odnosu na tradicionalne kreditne proizvode. Osmi slučaj je u vezi sa kolateralom, gde se planovi osiguranja takođe mogu koristiti kao obezbeđenje za tradicionalnije bankarske kredite, što predstavlja još jedan izvor čistog novca. Polisa, prvobitno kupljena na osnovu kriminalnih prihoda, može se dalje proslediti radi otplate avansa. Kolateral, gde se planovi osiguranja mogu tretirati kao kao obezbeđenje za tradicionalnije bankarske kredite, može predstavljati još jedan izvor čistog novca (deveti slučaj). U ovom slučaju polisa koja je finansirana iz kriminalnih prihoda može biti korišćena kao instrument otplate avansa. Dopunske premije (deseti slučaj) predstavljaju još jedan način koji perači novca primenjuju kada se na početku uspostavlja polisa osiguranja koju karakteriše niska početna premija koja zbog visine ne bi trebalo da privlači pažnju osiguravača ili regulatora. Nakon obezbeđivanja pravnog okvira polise, mogu se vršiti mnoge uplate kroz naknadne premije kako bi se izvršilo pranje novca.

Radna grupa za finansijske akcije (FATF) sve je više zabrinuta zbog izloženosti sektora osiguranja pranju novca. Međuvladina agencija je još 2018. godine utvrdila svoj pristup osiguranju zasnovan na riziku. Princip ovog pristupa je da procene rizika od pranja novca treba da odražavaju prirodu, veličinu i složenost poslovanja: od jednostavne procene za manje složene osiguravače i posrednike, do složenijeg posla za veće grupe. Drugim rečima, rad na finansijskoj regulativi i usklađenosti treba da bude srazmeran, prema mišljenju FATF-a. Potrebno je imati u vidu da i smernice agencije takođe naglašavaju važnost preuzimanja odgovornosti višeg rukovodstva za politike i procese sprečavanja pranja novca. Takođe, ukazuju na šire povezane rizike sa kojima se sektor suočava, uključujući mogućnost da se novac povučen iz polisa osiguranja može koristiti za finansiranje terorizma.

FATF ne postavlja sopstvene regulatorne standarde. Umesto toga, njegova uloga je da podrži i informiše države članice dok sprovedu regulatorne režime, obezbeđujući zajedničke standarde na međunarodnim tržištima. Međutim, iako ovo podržava saradnju između različitih zemalja i – barem donekle – informiše sličan regulatorni pristup, osiguravači i posrednici će morati jasno razumeti specifična pravila koja se primenjuju u svakoj jurisdikciji u kojoj posluju.

IV KRITIČNE TAČKE U INDUSTRIJI OSIGURANJA I PREPORUKE

Svet se brzo razvija, i na sceni se stalno pojavljuju novi akteri i načini plaćanja. U savremeno doba, perači novca koriste modernu nauku i tehnologiju, elektronsko bankarstvo i mogućnosti sajber prostora u funkciji obezbeđivanja aktivnosti što komplikovanijim po pitanju njihovog sprečavanja, otkrivanja i neutralizacije.³⁶ Stoga, sistem za sprečavanje pranja novca i finansiranja terorizma mora da se kontinuirano ažurira kako bi uspeo da u najvećoj meri održi korak sa inovacijama.

³⁶ G. Daniali, 29-38.

Da bi se miš uhvatio, koristi se sir, ali se postavlja pitanje na koji način je moguće uhvatiti pacova? "Nažalost po vlade i finansijska preduzeća, najuspešniji peraći novca su poput pacova - i ovi pacovi dostižu nove visine kreativnosti u svojoj potrazi za nezakonito stečenim dobicima"³⁷

Za sprečavanje pranja novca (AML) su neophodni robusni protokoli, a pod tim se podrazumeva nekoliko stvari: prvo, temeljna provera klijenata, drugo, praćenje transakcija i treće, poštovanje regulatornih okvira. U tom kontekstu se ističe da su adekvatne interne kontrole i jaka korporativna kultura takođe važni za sprečavanje i otkrivanje nezakonitih aktivnosti u industriji osiguranja. Kako sve više ljudi postaje svesno opasnosti od pranja novca i potrebe za koordinisanim odgovorom širom sveta, finansijske institucije, a među njima i osiguravajuće kompanije moraju da, pored ostalog, koriste najsavremenije tehnologije i podstiču komplajans kulturu.

Sistemi za sprečavanje pranja novca generalno nameću pravila čiji je fundament – rizik. Ovi sistemi moraju stalno da vode računa o novim trendovima i pretnjama kako bi ostali robusni. Kontinuirano praćenje transakcija je ključno za otkrivanje sumnjivog ponašanja. Osiguravači bi trebalo da koriste napredne sisteme za analitiku i praćenje transakcija koje se odnose na sumnjivo ponašanje kako bi se uočili neobični obrasci. Neki od njih koji se učestalo pojavljuju u praksi, jesu iznenadni zahtevi osiguranika za velike štete ili višestruka plaćanja premija u kratkom periodu. Današnji regulatori ulažu velike napore kako bi bili korak ispred ispred najnovijih prevara, dok se osiguravajuće kompanije intenzivno bore kako bi osigurale da mogu da identifikuju i onemoguće kriminalne aktivnosti, s jedne strane, kao i da obezbede usluge klijentima na što efikasniji način, s druge strane.

V ZAKLJUČAK

Prevara kao forma zarađivanja novca je uvek prolazne prirode. Prevare dovode do toga da finansijske institucije poput banaka i osiguranja uništavaju svoju reputaciju i imaju negativan uticaj na investitore. Kao i bankarski sektor, tako je i osiguranja postao veoma ranjiv, i oba su mete kriminalaca. Skandali sa pranjem novca mogu dovesti i do krivičnog gonjenja na sudu. Pranje novca i povezano finansiranje terorizma i organizovanog kriminala ostaju značajni problem. Šire gledno, proces pranja novca ima negativne posledice po razvoj konkurentnog tržišta i zdrave ekonomije. Zbog svega navedenog, ističe se značajna uloga tržišta osiguranja u celini u domenu borbe protiv pranja novca. Pritom treba imati u vidu da svako povećanje obima transakcija povlači za sobom i veći rizik od pranja novca i borbe protiv terorizma.

Osiguravači nastave da ulažu u programe za sprečavanje pranja novca, obučavaju svoje zaposlene. Pored toga, potrebno je i da prate najnovije trendove

³⁷ Laurie Newman, "Making the most of anti-money laundering systems", *Journal of Superannuation Management*, No.2/2007, 31-34.

pranja novca kako bi se efikasno upravljalo rizikom od pranja novca i finansiranja terorizma. Pranje novca i korišćenje prihoda od kriminala su aktivnosti duboko utka-
ne u ekonomske, političke i društvene probleme nove ere, tako da je ovom pitanju
potrebno posvetiti još veću pažnju od strane, kako regulatora, tako i akademske za-
jednice, posebno u delu koji se odnosi na razvoj novih modela za efikasno upravljanje
rizikom od pranja novca, kako u nacionalnim okvirima, tako i na globalnom nivou.

Literatura

- Garner, B. A., *Black's Law Dictionary*, Thomson West, Eagan, 2019.
- Ghorban Daniali, "E-money Laundering Prevention", *New Marketing Research Journal*, Special Issue, 2014, 29-38.
- Jeffrey, S., "Money laundering: emerging threats and trends", *Journal of Money Laundering Control*, No. 1/2012, 41-54.
- Knežević, S., "Faktori kvaliteta finansijskog izveštavanja osiguravajućih društava", Referat na XLII Simpozijumu Saveza računovođa i revizora Srbije, Zlatibor, 2011, 411-427.
- Lijuan, M., "Anti-Money Laundering", *Dictionary of Contemporary Chinese Economics* (ed. Yinxing, H), Singapore, 2025.
- Milojević, S., Knežević, S., Šebek, V., "Upravljanje rizikom od prevara u osiguranju", *Tokovi osiguranja*, br. 4/2024, 938-961.
- Mulig, E. V., & Smith, M., "Understanding and preventing money laundering", *Internal auditing*, No. 5/2004, 22-25.
- Nazzari, M., Reuter, P., "How well does the money laundering control system work?", *Crime and Justice*, No. 1/2025, 67-152.
- Newman, L., "Making the most of anti-money laundering systems", *Journal of Superannuation Management*, No. 2/2007, 31-34.
- Palshikar, G. K., "Detecting Frauds and Money Laundering: A Tutorial", *Big Data Analytics* (eds. Srinath Srinivasa, Sameep Mehta), Springer, Cham, 2014.
- Ping, H., "A typological study on money laundering", *Journal of Money Laundering Control*, No. 1/2010, 15-32.
- Reznik, O., Utkina, M., Bondarenko, O. "Financial intelligence (monitoring) as an effective way in the field of combating money laundering." *Journal of Money Laundering Control*, No. 1/2023, 94-105.
- Sanomat, H., *Criminals Rush for Euros*, Helsinki, Finland, 2001.
- Savona, E. U., De Feo, M. A., "International money laundering trends and prevention/control policie.", *Responding to Money Laundering: International Perspectives* (ed. E. Savona), Harwood Academic, Amsterdam, 1997, 9-71.

- Sharman, J. C., "Power and discourse in policy diffusion: anti-Money laundering in developing states", *International Studies Quarterly*, No. 3/2008, 635-656.
- Simser, J., "Money Laundering: Emerging Threats and Trends", *Journal of Money Laundering Control*, No. 1/2012, 41-54.
- Smith, D., "Common Money Laundering Schemes and Red Flags or Warnings of It", *Money Laundering, Terrorist Financing and Virtual Assets: Cases and Materials*, Springer, Cham 2024, 35-46.
- Stumbauer, S., "Basics of Anti-Money Laundering Compliance", *The Next Wave of Global Anti-Money Laundering Enforcement*, Palgrave Macmillan, Cham, 2024, 21-26.
- Sullivan, K., "Fraud and Anti-Money Laundering. In: Anti-Money Laundering in a Nutshell", *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers* (ed. Kevin Sullivan), Apress, Berkeley, CA, 2023, 219-229.

UDK 343.85:347.764
10.5937/TokOsig2602260M

Professor Stefan V. Milojević, PhD¹
Professor Snežana P. Knežević, PhD²
Aleksandra Mitrović³

MONEY LAUNDERING IN THE INSURANCE INDUSTRY

REVIEW SCIENTIFIC PAPER

Abstract

Money laundering is a highly complex activity aimed at concealing the source and nature of illicit funds so that they appear legitimate and subsequently become usable and transferable, thereby posing a serious threat to the financial system. In addition to its primary purpose, insurance can also be used as a financial instrument in money laundering. Money laundering and terrorist financing have become opportunities for criminals to legitimize illicit proceeds derived from insurance-related activities. This study aims to identify potential indicators that may facilitate money laundering and to examine possible prevention mechanisms. Combating money laundering as a criminal activity in the insurance industry is a continuous undertaking that requires constant adaptability, as money laundering methods are evolving and the activities through which laundering is carried out are becoming increasingly sophisticated. The findings indicate that effective prevention, as the first line of defense against money laundering in the insurance sector, can be achieved through regulatory oversight, the implementation of advanced technological solutions, and continuous employee training on money laundering risks and compliance procedures. It is concluded that the insurance industry continues to

¹ Associate Professor, Educons University, Faculty of Business Economics, Email: stefan.milojevic@educons.edu.rs. ORCID ID 0000-0001-6240-6776.

² Full Professor, University of Belgrade, Faculty of Organizational Sciences, Email: snezana.knezevic@fon.bg.ac.rs. ORCID ID 0000 0001 9833 7274.

³ Associate Professor, University of Kragujevac, Faculty of Hotel Management and Tourism in Vrnjačka Banja, Email: aleksandra.stankovic@kg.ac.rs ORCID ID 0000-00028302-0853.

Paper received: 26.3.2026.

Paper accepted: 11.6.2026.

represent a significant risk channel that requires ongoing improvement of control and supervisory systems.

Keywords: insurance, risk, money laundering, compliance.

JEL Classification: G22, K42, G18.

I INTRODUCTION

Money laundering (ML; or “blanqueo” in Spanish, “blanchiment” in French, “riciclaggio” in Italian, and similar terms in other languages) is widely understood as the process of concealing the criminal origin of assets and investments or the illegal nature of financial transactions.⁴ It represents the process of generating large amounts of capital acquired through unlawful or unethical activities associated with serious criminal offenses such as drug trafficking, organized crime, terrorism, and similar crimes.⁵ According to another definition, money laundering may be defined as a technique used by criminals to conceal the origin of illicit proceeds with the intention of enjoying their “cleaned” money without interference from either rival criminal groups or law enforcement authorities.⁶

As noted above, money laundering can be defined in different ways depending on the source. Although the definitions used by various regulatory bodies, criminal laws, and law enforcement agencies are all valid, each focuses primarily on its own area of concern, whether criminal aspects, accounting aspects, or the unlawful nature of the activities involved.

Internet-based money laundering is so complex that it is often difficult to determine where it actually takes place. It is also challenging to identify the authority responsible for investigating and prosecuting transnational criminal activities.⁷

Criminals engage in money laundering activities in order to obstruct investigations and avoid criminal prosecution. The precise definition of money laundering varies across jurisdictions. Money laundering transforms illegal money (illicit funds) into assets that appear legitimate. It can be viewed as a complex process consisting of three stages: placement, layering, and integration of illicit proceeds (Figure 1).

⁴ Ernesto Ugo Savona, Michale De Feo, “International money laundering trends and prevention/control policies”, *Responding to Money Laundering: International Perspectives* (ed. E. Savona), Harwood Academic, Amsterdam, 1997, 9-71.

⁵ Ayush Kumar *et al.*, “Fraud Detection in Anti-money Laundering System Using Machine Learning Techniques”, *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences. Algorithms for Intelligent Systems* (ed. Mayank Dave *et al.*) Springer, Singapore, 2020.

⁶ Jeffrey Simser, “Money Laundering: Emerging Threats and Trends”, *Journal of Money Laundering Control*, No. 1/2012, 41-54.

⁷ Ping He, “A typological study on money laundering”, *Journal of Money Laundering Control*, No. 1/2010, 15-32.

Although it is an ancient phenomenon, money laundering was first criminalized only in 1986.⁸

Figure 1. Basic Stages of the Money Laundering Process⁵

<u>Placement</u>	<u>Layering</u>	<u>Integration</u>
Cash deposited into bank (often with complicity of staff or mixed with proceeds of legitimate businesses)	Funds are transferred abroad, often to shell companies or disguised as proceeds of legitimate business.	False loan repayment or forged invoices used as cover for laundered money
Cash physically transported out of country.	Deposits made in overseas banking system or closely-held bank.	Complex web of transfers (both domestic and international) makes tracing original source of funds virtually impossible.
Cash used to buy high value goods, property, or business assets.	Previously purchased goods and assets are sold to obtain cash.	Income from property or legitimate business assets appears "clean."

Source: Elizabeth Vallery Mulig, Murphy Smith, "Understanding and preventing money laundering", *Internal auditing*, No. 5/2008, 22-25.

Money laundering is frequently associated with narcotics trafficking, corruption, prostitution, illegal arms trading, tax evasion, and terrorist financing. The process of identifying and combating such activities is referred to as Anti-Money Laundering (AML). Illicit assets may take the form of insurance policies, bank deposits, or real estate. Money laundering activities are not limited to financial institutions, as non-financial sectors such as travel agencies, the real estate industry, casinos, and gambling operations are also increasingly used for laundering illicit funds. The nature of money laundering in the insurance industry, however, differs from that observed in other sectors. The insurance sector is primarily composed of insurance companies, insurance agencies, brokers, and reinsurers. The specific characteristics of insurance companies stem from the fundamental nature of their operations and the risks inherent in their business activities.⁹

⁸ Jason Sharman. "Power and discourse in policy diffusion: anti-Money laundering in developing states", *International Studies Quarterly*, No. 3/2008, 635-656.

⁹ Snežana Knežević, "Factors Affecting the Quality of Financial Reporting in Insurance Companies", Paper presented at the 42nd Symposium of the Association of Accountants and Auditors of Serbia, Zlatibor, Serbia, 411-427.

For anti-money laundering efforts to be effective, an environment that encourages honest and transparent reporting must exist. Legal authorities, policymakers, and the public must provide adequate support. In its efforts to promote such an environment, the International Federation of Accountants (IFAC) encourages its member bodies to establish collaborative relationships with legislative and regulatory authorities at both the corporate and governmental levels.

On a global scale, money laundering imposes substantial costs on the world economy by undermining the efficient functioning of national economies and fostering poor economic policies. As a result, financial markets gradually become corrupted, public confidence in the international financial system is weakened, and negative consequences arise for global economic growth. For these reasons, concerns regarding money laundering originate from numerous directions.¹⁰

Money laundering represents a systemic risk to the financial and economic sectors, as well as to the national security of all countries.¹¹ Numerous domestic and international organizations are engaged in combating money laundering. The United States has enacted several stringent anti-money laundering laws, including:

- The Anti-Drug Abuse Act of 1988;
- The Crime Control Act of 1990;
- The Annunzio-Wylie Anti-Money Laundering Act of 1992;
- The Money Laundering Suppression Act of 1994;
- The Antiterrorism Act of 1995;
- New reporting requirements for financial institutions were introduced in 1996; and
- The USA PATRIOT Act (USAPA) of 2001.

International efforts to combat money laundering are reflected in the activities of the World Bank, international agreements, and the Financial Action Task Force (FATF). The World Bank promotes measures aimed at preventing or slowing the flow of illicit funds into emerging markets. International initiatives include the Vienna Convention, the 1990 Council of Europe Convention, the Basel Statement of Principles, European Union Directives, and resolutions issued by the International Organization of Securities Commissions (IOSCO).¹²

The evolution of various regulations and amendments introduced by regulators has been inevitable, given the exposure of insurers to increasingly sophisticated methods and mechanisms of financial crime. A key role in establishing internationally harmonized anti-money laundering and counter-terrorist financing

¹⁰ Helsingin Sanomat. *Criminals Rush for Euros*. Helsinki, Finland, 2001.

¹¹ Oleg Reznik, Maryna Utkina, Olha Bondarenko, „Financial intelligence (monitoring) as an effective way in the field of combating money laundering”, *Journal of Money Laundering Control*, No. 1/2023, 94-105.

¹² Elizabeth Vallery Mulig, Murphy Smith, “Understanding and preventing money laundering”, *Internal auditing*, No. 5/2008, 22-25.

(AML/CFT) standards is played by the Financial Action Task Force (FATF). FATF develops and promotes international AML/CFT standards, fosters the political commitment necessary for the implementation of regional and national regulatory reforms, and evaluates the effectiveness of measures adopted by individual countries.

In Serbia, the primary AML/CFT legislation is the Law on the Prevention of Money Laundering and Terrorist Financing.¹³ This law prescribes the actions and measures undertaken to prevent and detect money laundering and terrorist financing. In addition, it regulates the jurisdiction of the Administration for the Prevention of Money Laundering and the responsibilities of other authorities involved in implementing the provisions of the Law, including oversight of its application. Pursuant to Article 4 of the Law, obliged entities include insurance companies licensed to conduct life insurance business, insurance brokerage companies engaged in life insurance intermediation, insurance agency companies, and insurance agents authorized to perform life insurance activities, except for those whose activities are legally carried out under the responsibility of an insurance company.

FATF identifies several warning signs that may alert companies to potential money laundering activities and groups them into several categories:

Table 1. Red Flags (Indicators of Potential Money Laundering)

Red Flag Category	Example
Customer Behavior	The customer is excessively secretive or avoids providing information regarding their identity.
Source of Funds	The customer uses multiple bank accounts without a justified business reason.
Unnecessary Use of Legal Professionals or Complex Legal Structures	The customer engages a law firm to establish multiple offshore companies and trusts in different jurisdictions.
Nature of the Engagement	The customer participates in transactions that are inconsistent with their usual business activities.
Geographic Risk	The customer originates from, or conducts business with, a jurisdiction known for high levels of corruption, weak anti-money laundering enforcement, or international sanctions.

Source: Adapted from FATF Guidance.

A suspicious transaction is any intended or completed transaction for which an employee knows or has reasonable grounds to suspect that the property or funds originate from a predicate money laundering offense or are related to terrorist financing.

¹³ Law on the Prevention of Money Laundering and Terrorist Financing, *Official Gazette of the Republic of Serbia*, Nos. 113/2017, 91/2019, 153/2020, 92/2023, 94/2024, and 19/2025.

Drug trafficking is the principal predicate offense for money laundering, and the risk of money laundering varies depending on the level of drug-related activity.¹⁴

Any bank employee, regardless of position, who identifies grounds for suspicion of money laundering or terrorist financing should immediately notify the designated local anti-money laundering officer, who is responsible for providing professional assistance in assessing the suspicion.

There are numerous general warning indicators of potential money laundering. Some additional examples include:

- The customer makes detailed inquiries with professionals regarding methods of avoiding the reporting of transactions to the Financial Intelligence Unit (FIU);
- The customer displays signs of fear or nervousness;
- The customer possesses unusually extensive knowledge of anti-money laundering and counter-terrorist financing regulations and requirements;
- Control over funds in the same account is granted to one or more individuals who clearly have no legitimate relationship with the account holder;
- A business relationship is established with a legal entity known to share the same registered office and legal representative as another legal entity;
- No logical connection can be identified between the transactions performed and the customer's business activities;
- The customer conducts cash and non-cash transactions in amounts slightly below the reporting threshold applicable to the Financial Intelligence Unit;
- The customer deposits unusually large amounts of cash that are disproportionate to their normal business activities;
- The customer uses a business account in a manner inconsistent with the purpose for which the account was opened;
- The customer accesses a safe deposit box immediately before or after conducting a cash-related transaction;
- The business relationship is established by an individual or legal entity that may be linked to a terrorist organization.

Particular emphasis should be placed on the importance of harmonizing cyberspace and e-government systems across related institutions, including banks, stock exchanges, insurance companies, national civil registration authorities, property and document registration agencies, and business registration authorities, in order to strengthen efforts to combat electronic money laundering. Government officials should seriously consider developing updated legislation and regulations, strengthening infrastructure, fostering public acceptance, and enhancing

¹⁴ J. Simser, 41–54.

international cooperation.¹⁵ The increasing integration of global financial systems and the removal of barriers to the free movement of capital create favorable conditions for criminal organizations engaged in money laundering. These developments facilitate the laundering of illicit proceeds and make financial tracking more difficult. It is well known that fraudulent insurance claims have long represented one of the most common forms of abuse within the insurance industry. Given the continuously growing volume of financial transactions, the insurance sector has increasingly been used by money launderers to legitimize proceeds derived from criminal activities.

The remainder of this paper is organized as follows. Section 2 examines insurance fraud and the phenomenon of money laundering. Section 3 discusses the specific characteristics of money laundering within the insurance industry. Section 4 identifies critical issues within the insurance sector and provides relevant recommendations, while Section 5 concludes the paper.

II INSURANCE FRAUD AND THE PHENOMENON OF MONEY LAUNDERING

According to *Black's Law Dictionary*,¹⁶ fraud is defined as "a knowing misrepresentation of the truth or concealment of a material fact to induce another person to act to his or her detriment." The four essential elements of fraud are: (1) a false representation concerning (2) a material fact that is (3) intentionally made with (4) the intent to deceive. Today, fraud is prevalent across all sectors of the economy, including banking and financial services, insurance, telecommunications, retail, transportation, and government organizations, differing in both scale and complexity.¹⁷ Insurance fraud represents a significant challenge for insurance companies, as it results in financial losses, market destabilization, and a loss of customer confidence. In order to protect individual insurance companies on the one hand and ensure the sustainability of the insurance industry on the other, effective fraud risk management is essential.¹⁸

For the criminal offense of money laundering to exist, there must first be a predicate offense. Money laundering cannot be considered independently of the predicate crime that generates the assets subsequently laundered. In this context,

¹⁵ Ghorban Daniali, "E-money laundering prevention", *New Marketing Research Journal*, Special Issue, 2014, 29-38.

¹⁶ Bryan A. Garner, *Black's Law Dictionary*, Thomson West, Eagan, 2019.

¹⁷ Girish Keshav Palshikar, "Detecting Frauds and Money Laundering: A Tutorial", *Big Data Analytics* (eds. Srinath Srinivasa, Sameep Mehta), Springer, Cham, 2014.

¹⁸ Stefan Milojević, Snežana Knežević, Vladimir Šebek, "Upravljanje rizikom od prevara u osiguranju", *Tokovi osiguranja*, No. 4/2024, 938-961.

the 6th Anti-Money Laundering Directive (6AMLD)¹⁹ provides a harmonized list of predicate offenses which, in addition to traditional money laundering-related crimes such as drug trafficking, human trafficking, illicit arms trafficking, corruption, and fraud, also include tax offenses, environmental crime, and cybercrime. Fraud is one of the most common predicate offenses leading to money laundering. Since financial institutions typically maintain both fraud investigation units and anti-money laundering units, it is logical that these two functions operate in close coordination and alignment.²⁰ The term FRAML is commonly used to describe the integration of fraud prevention and anti-money laundering activities (FRAUD + AML).

Two important questions arise in this context: who commits insurance fraud, and what forms of fraud are most prevalent within the insurance industry? According to an FBI report,²¹ The U.S. insurance industry loses approximately USD 40 billion annually to fraud in the non-health insurance sector alone. Common perpetrators of insurance fraud include dishonest policyholders, individuals employed within the insurance industry (such as agents, brokers, and company executives), as well as loosely organized networks of corrupt medical professionals and attorneys who use their expertise to circumvent anti-fraud measures implemented by insurance companies.²²

Numerous forms of fraud are present within the insurance industry. Customers willing to accept unfavorable policies, the involvement of undisclosed parties, exaggerated claims, and false or fraudulent claims are among the most common forms of insurance fraud. Claims involving fabricated deaths or alleged memory loss are frequent forms of fraud in life insurance. Other fraudulent practices include premium non-payment, disproportionate commissions, insurance policies issued by non-existent companies, unreliable medical documentation, backdated policies, extortion through document falsification, and even kidnapping and murder schemes associated with insurance benefits.

According to the National Insurance Crime Bureau (NICB), general indicators of insurance fraud related to inventory and property losses may include the following:²³

- Inventory loss/property fraud;
- The insured has recently separated or divorced;
- Invoices are submitted weeks or months after the work was performed;

¹⁹ Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. available at: <https://eur-lex.europa.eu/eli/dir/2018/1673/oj/eng>, accessed 3.3.2026.

²⁰ Kelvin Sullivan, "Fraud and Anti-Money Laundering. In: Anti-Money Laundering in a Nutshell", *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers* (ed. Kevin Sullivan), Apress, Berkeley, CA, 2023, 219-229.

²¹ <http://www.fbi.gov/stats-services/publications/insurance-fraud>, accessed 2.2.2026.

²² Investigating Insurance Fraud: A \$30-Billion-a-Year Racket, available at: <https://www.fbi.gov/news/stories/investigating-insurance-fraud>, accessed 3.5.2026.

²³ Indicators of Property Fraud: Individuals & Professionals Involved/Circumstances & Documents Detection -The First Line of Defence.

- The policy is cancelled shortly after a claim is filed, often due to non-payment of premiums;
- Reported losses are inconsistent with the insured's occupation and/or income;
- Losses involve substantial amounts of cash;
- Inventory loss/fire-related fraud;
- Pets were not present at the time of the fire;
- Losses involve old, obsolete, unsellable inventory or illegal chemicals and materials;
- The insured or the insured's business is experiencing financial difficulties (bankruptcy or foreclosure);
- The investigation reveals no remains of non-combustible items allegedly lost in the incident (coins, firearms collections, jewelry, etc.);
- The fire occurred late at night, after 11:00 p.m.;
- Fire department reports indicate that the cause of the fire was incendiary, suspicious, or undetermined;
- Inventory loss resulting from burglary or theft;
- Commercial losses occur at locations with little or no security measures;
- Claim-related inventory loss processes;
- The insured's reported inventory losses differ significantly from police reports;
- The insured submits receipts without a store logo (blank receipts);
- The insured submits two different receipts displaying identical handwriting or fonts;
- The insured submits a single receipt containing multiple handwriting styles or fonts.

Money laundering is often referred to as the "dirty little secret" of the financial world.²⁴ Smith (2024)²⁵ notes that common money laundering schemes include shell companies, offshore accounts, gambling activities, cryptocurrencies, transactions with unusual characteristics, and politically exposed persons (PEPs),²⁶ geographic risk factors, opaque beneficial ownership structures, and sudden changes in transaction instructions. The global financial system has become increasingly interconnected. Public exposure and reputational pressure have compelled insurance companies, among other financial institutions, to strengthen their compliance systems and

²⁴ Sven Stumbauer, "Basics of Anti-Money Laundering Compliance", *The Next Wave of Global Anti-Money Laundering Enforcement*, Palgrave Macmillan, Cham, 2024, 21-26.

²⁵ Dunan Smith, "Common Money Laundering Schemes and Red Flags or Warnings of It", *Money Laundering, Terrorist Financing and Virtual Assets: Cases and Materials*, Springer, Cham 2024, 35-46.

²⁶ A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function. Many such individuals occupy positions that may be abused for the purpose of laundering illicit funds or engaging in other unlawful activities, such as corruption or bribery. Reference: Financial Action Task Force (FATF). Guidance: Politically Exposed Persons (Recommendations 12 and 22). Available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html>, accessed 12.3.2026.

invest in new technologies capable of detecting and potentially preventing money laundering activities.²⁷ Consequently, the transition from a reactive to a proactive approach in managing money laundering and terrorist financing risks has become a necessity in today's highly dynamic environment.

III MONEY LAUNDERING IN THE INSURANCE INDUSTRY

From a general perspective, "money laundering is a term used to describe a scheme in which criminals attempt to conceal the identity, original ownership, and destination of money obtained through criminal activity."²⁸ Money laundering frequently involves a complex series of transactions and numerous financial institutions operating across different sectors. Non-bank financial entities, such as currency exchange services, check-cashing businesses, insurance companies, intermediaries, and merchants, are increasingly being used as instruments by individuals engaged in money laundering activities.

Money laundering through insurance institutions serves to conceal the source and nature of illicit proceeds, as well as profits generated through the purchase, modification, surrender of insurance policies, and the submission of insurance claims, thereby preventing effective tracing by authorities.²⁹ Insurance institutions have been extensively utilized by money launderers, raising the question of why they are particularly attractive for such purposes. Although there are numerous reasons, the key determinants generally lie in the characteristics of insurance operations and the relatively limited intervention of legal authorities within this market.

Methods of money laundering include cash smuggling, the use of banks or insurance companies, and the establishment of shell companies or front companies. Today, criminals also rely on real estate transactions, lotteries, international trade, and offshore companies to launder illicit funds. In some cases, money launderers exploit the services of lawyers and accountants. With the widespread adoption of electronic money and internet-based financial services, criminals have adapted their strategies accordingly. Consequently, an important question arises as to whether money launderers have shifted part of their activities from banks to insurance companies.

Insurance products, particularly life insurance products, provide a highly attractive and relatively simple mechanism for money laundering. Investment-linked life insurance products are especially vulnerable. Acharya (2015)³⁰ further notes

²⁷ S. Stumbauer.

²⁸ M. Lijuan, "Anti-Money Laundering", *Dictionary of Contemporary Chinese Economics* (ed. Hong Yinxing), Springer, Singapore, 2025.

²⁹ H. Ping, 15–32.

³⁰ Acharya Suman, Money Laundering (ML) and Terrorism Financing (TF) in the Insurance Market: A Risk and Vulnerability, available at: <https://ssrn.com/abstract=2604560> or <http://dx.doi.org/10.2139/ssrn.2604560>, 11. 6. 2026.

that although the life insurance sector is highly exposed, significant risks of money laundering and terrorist financing are also present in general insurance, reinsurance, insurance intermediaries, and insurance agents.

According to the Financial Crimes Enforcement Network (FinCEN),³¹ "The most significant money laundering and terrorist financing risks within the insurance industry are associated with life insurance and annuity products, as these products enable customers to place substantial amounts of funds into the financial system and transfer them seamlessly in order to conceal their true origin."

Transactions that should attract the attention of AML professionals include:

- Large premium payments made in cash;
- Unusual policy structures;
- Frequent changes in beneficiary designations; and
- Transactions involving high-risk geographic regions.

Within the insurance sector, it is essential to adopt a risk-based approach. Insurance companies are expected to assess money laundering risks associated with their business operations and customers and to implement measures proportionate to those risks. For example, high-risk customers or transactions may require enhanced Customer Due Diligence (CDD)³² and closer monitoring.

For the successful prevention of money laundering, it is important that all participants in the financial sector consistently apply Know Your Customer (KYC) procedures as well as customer monitoring and Customer Due Diligence (CDD)³³ measures. KYC and AML are powerful complementary mechanisms and essential components for insurance companies seeking to protect themselves from fraud and financial crime. Both involve verifying the identity and legitimacy of individuals and organizations through rigorous screening procedures. In itself, this makes it considerably more difficult for criminals to operate. Furthermore, AML controls help trace the movement of funds, identify their origin, and understand how they are used, enabling organizations to ensure that they are not being exploited for money laundering purposes.³⁴

³¹ Financial Crimes Enforcement Network, available at: <https://www.fincen.gov/>, 4.4.2026.

³² There are three categories of measures applied within the anti-money laundering framework. Simplified Due Diligence (SDD) measures are applied to low-risk customers, Standard Due Diligence (CDD) measures are applied to medium-risk customers, while Enhanced Due Diligence (EDD) measures are reserved for high-risk customers.

³³ Mirko Nazzari, Peter Reuter, "How well does the money laundering control system work?", *Crime and Justice*, No. 1/2025, 67-152.

³⁴ An interesting example can be found in Mauritius, where every bank and insurance company was required to contact all account holders and policyholders and request that they appear in person with identification documents. This requirement applied even to the Prime Minister, who publicly complained about the inconvenience. Failure to comply resulted in accounts and insurance policies being classified as "frozen." J. Sharman. 635-656.

Insurers may be vulnerable to AML risks in various segments of their operations.³⁵ The first case (general insurance) occurs when high-value assets purchased with proceeds derived from criminal activities are insured and subsequently used as the basis for fraudulent claims for compensation. In this way, indemnities paid by insurers are transformed into a seemingly legitimate source of funds. The second case involves the purchase of single-premium insurance policies, which provide individuals engaged in criminal activities with an opportunity to transfer substantial amounts of money into the financial services ecosystem. The third case relates to annuity contracts, under which insurance plans provide a regular stream of income in exchange for an upfront lump-sum cash payment. This arrangement enables money launderers to convert part of their illicit funds into a steady flow of legitimate income. The fourth case concerns the cooling-off period. Financial regulations often require insurers to refund premiums if a policyholder decides to cancel a policy within a specified period after its purchase. Such refunds effectively provide money launderers with a legitimate source of funds. The fifth case relates to surrender clauses. Many insurance policies, including savings plans, allow policyholders to surrender their contracts before maturity, although this usually involves a financial penalty. For money launderers, such clauses provide a mechanism for obtaining legitimate funds even when the policy was originally purchased using illicit proceeds. The sixth case involves policy sales. Many insurance products now have a thriving—and entirely legitimate—secondary market where coverage can be sold. This represents an attractive option for money launderers because they can sell their policies for a lump-sum payment originating from legitimate sources. The seventh case concerns policy loans. Some insurers are willing to grant loans secured by the value of life insurance policies, provided that the policy serves as collateral throughout the lending process. For money launderers, this represents a straightforward means of obtaining a lump sum of cash from a legitimate source. This opportunity is further enhanced by the fact that such loans are often subject to less scrutiny than traditional lending products. The eighth case relates to collateralization, whereby insurance policies may also be used as security for conventional bank loans, thereby creating another source of apparently legitimate funds. A policy originally purchased using criminal proceeds may subsequently be assigned to repay an advance. Collateralization, where insurance policies serve as security for traditional banking loans, may also constitute another source of clean money (the ninth case). In such circumstances, a policy financed through criminal proceeds may be used as an instrument for loan repayment. Additional premium payments (the tenth case) represent another method commonly employed by money launderers. Initially, an insurance policy is established with a low premium that, due to its small value,

³⁵ Where insurers may be vulnerable to AML risk, available at: <https://kyc360.com/platform>, 2.2.2026.

is unlikely to attract the attention of insurers or regulators. Once the legal framework of the policy has been established, multiple subsequent premium payments may be made in order to launder illicit funds.

The Financial Action Task Force (FATF) has become increasingly concerned about the exposure of the insurance sector to money laundering risks. As early as 2018, the intergovernmental organization established its risk-based approach for the insurance industry. The underlying principle of this approach is that money laundering risk assessments should reflect the nature, size, and complexity of the business, ranging from relatively simple assessments for smaller insurers and intermediaries to considerably more sophisticated frameworks for larger insurance groups. In other words, according to FATF, regulatory compliance and financial supervision efforts should be proportionate to the level of risk involved. It should also be noted that FATF guidance emphasizes the importance of senior management assuming responsibility for anti-money laundering policies and procedures. Furthermore, the guidance highlights broader risks facing the sector, including the possibility that funds withdrawn from insurance policies may ultimately be used to finance terrorist activities.

FATF does not establish its own regulatory standards. Rather, its role is to support and guide member states in implementing regulatory regimes while promoting common standards across international markets. Although this facilitates cooperation among different countries and, to some extent, encourages a harmonized regulatory approach, insurers and intermediaries must clearly understand and comply with the specific rules applicable in every jurisdiction in which they operate.

IV CRITICAL ISSUES IN THE INSURANCE INDUSTRY AND RECOMMENDATIONS

The world is evolving rapidly, and new market participants and payment methods are constantly emerging. In the modern era, money launderers make use of advanced science and technology, electronic banking, and the opportunities provided by cyberspace to make their activities increasingly difficult to prevent, detect, and neutralize.³⁶ Consequently, anti-money laundering and counter-terrorist financing systems must be continuously updated in order to keep pace with ongoing innovations.

To catch a mouse, one uses cheese; however, the question remains how to catch a rat. As Newman (2007) aptly noted, "Unfortunately for governments and financial institutions, the most successful money launderers are like rats—and these rats continue to reach new heights of creativity in their pursuit of illicit gains."³⁷

³⁶ G. Daniali, 29-38.

³⁷ Laurie Newman, "Making the most of anti-money laundering systems", *Journal of Superannuation Management*, No. 2/2007, 31-34.

Robust anti-money laundering (AML) protocols are essential. These protocols encompass several key elements: first, thorough customer due diligence; second, transaction monitoring; and third, compliance with regulatory requirements. In this context, it should be emphasized that adequate internal controls and a strong corporate culture are also critical for preventing and detecting illegal activities within the insurance industry. As awareness of the dangers of money laundering and the need for a coordinated global response continues to grow, financial institutions, including insurance companies, must employ state-of-the-art technologies and foster a strong compliance culture.

Anti-money laundering systems are generally based on a risk-oriented approach. Such systems must continuously adapt to emerging trends and threats in order to remain effective and resilient. Ongoing transaction monitoring is essential for identifying suspicious behavior. Insurers should employ advanced analytics and transaction-monitoring systems capable of detecting unusual patterns. Common examples encountered in practice include sudden claims for substantial losses and multiple premium payments made within a short period of time. Regulators today are making significant efforts to stay ahead of the latest fraud schemes, while insurance companies are striving to ensure that they can identify and prevent criminal activities on the one hand and provide efficient services to their customers on the other.

V CONCLUSION

Fraud as a means of generating income is inherently unsustainable. Fraudulent activities damage the reputation of financial institutions such as banks and insurance companies and negatively affect investor confidence. Like the banking sector, the insurance industry has become highly vulnerable, and both sectors have become attractive targets for criminals. Money laundering scandals may also result in criminal prosecution and legal sanctions. Money laundering and the associated financing of terrorism and organized crime remain significant global challenges. More broadly, the money laundering process has adverse consequences for the development of competitive markets and healthy economies. For this reason, the insurance market plays an important role in the overall fight against money laundering. It should also be recognized that every increase in the volume of financial transactions inevitably leads to a greater risk of money laundering and terrorist financing.

Insurers must continue investing in anti-money laundering programs and the training of their employees. In addition, they must closely monitor emerging money laundering trends in order to manage money laundering and terrorist financing risks effectively. Money laundering and the use of proceeds derived from criminal activities are deeply embedded in the economic, political, and social challenges of the modern era. Therefore, greater attention should be devoted to this issue by

both regulators and the academic community, particularly in the development of new models for the effective management of money laundering risks at both the national and global levels.

Literature

- Acharya, A., *Anti-Money Laundering and Insurance Sector Risks*, 2015.
- Garner, B. A., *Black's Law Dictionary*, Thomson West, 2019.
- Daniali, G., "E-Money Laundering Prevention", *New Marketing Research Journal*, Special Issue, 2014, 29–38.
- Knežević, S., "Faktori kvaliteta finansijskog izveštavanja osiguravajućih društava.", Proceedings of the XLII Symposium of the Association of Accountants and Auditors of Serbia, Zlatibor, 2011, 411–427.
- Lijuan, M., "Anti-Money Laundering", *Dictionary of Contemporary Chinese Economics* (ed. H. Yinxiang), Singapore, Springer, 2025.
- Milojević, S., Knežević, S., Šebek, V., "Upravljanje rizikom od prevara u osiguranju?", *Tokovi osiguranja*, No. 4/2024, 938–961.
- Mulig, E. V., & Smith, M., "Understanding and Preventing Money Laundering", *Internal Auditing*, No. 19/2008, 22–25.
- Nazzari, M., Reuter, P., "How Well Does the Money Laundering Control System Work?", *Crime and Justice*, No. 1/2024, 67–152.
- Newman, L., "Making the Most of Anti-Money Laundering Systems", *Journal of Superannuation Management*, No. 1/2007, 31–34.
- Palshikar, G. K., "Detecting Frauds and Money Laundering: A Tutorial", *Big Data Analytics* (eds. Srinath Srinivasa, Sameep Mehta), Springer, Cham, 2014.
- Ping, H., "A Typological Study on Money Laundering", *Journal of Money Laundering Control*, No. 1/2010, 15–32.
- Reznik, O., Utkina, M., & Bondarenko, O., "Financial Intelligence (Monitoring) as an Effective Way in the Field of Combating Money Laundering", *Journal of Money Laundering Control*, No. 1/2023, 94–105.
- Sanomat, H., *Criminals Rush for Euros*, Helsinki, Finland, 2001.
- Savona, E. U., De Feo, M. A., *International Money Laundering Trends and Prevention/Control Policies. In Responding to Money Laundering: International Perspectives* 9–71. Amsterdam: Harwood Academic, 1997.
- Sharman, J. C., "Power and Discourse in Policy Diffusion: Anti-Money Laundering in Developing States", *International Studies Quarterly*, No. 3/2008, 635–656.
- Smith, D., *Common Money Laundering Schemes and Red Flags or Warnings of It. In Money Laundering, Terrorist Financing and Virtual Assets: Cases and Materials*, Cham: Springer Nature Switzerland, 2024.

- Stumbauer, S., *Basics of Anti-Money Laundering Compliance. In The Next Wave of Global Anti-Money Laundering Enforcement*, Cham: Palgrave Macmillan, 2025.
- Sullivan, K., "Fraud and Anti-Money Laundering. In: *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers* (ed. Kevin Sullivan), Apress, Berkeley, CA, 2023, 219-229.

Preveli: autori