UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

IZBIRA PROGRAMSKE REŠITVE ZA PREPREČEVANJE PRANJA DENARJA IN FINANCIRANJA TERORIZMA

Ljubljana, avgust 2016 MATJAŽ ŠPILAK

IZJAVA O AVTORSTVU

Podpisani Matjaž Špilak, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Izbira programske rešitve za preprečevanje pranja denarja in financiranja terorizma, pripravljenega v sodelovanju s svetovalcem prof. dr. Andrejem Kovačičem.

IZJAVLJAM

1. da sem predloženo delo pripravil/-a samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel/-a, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;

7. da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študenta(-ke):_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Pranje denarja in financiranje terorizma predstavljata veliko grožnjo miru v svetu. Če samo pogledamo velike količine opranega denarja, kar je lahko posledica velikega povpraševanja po prepovedanih drogah ali pa število terorističnih napadov v zadnjem obdobju, je to dober kazalnik, da je treba področje preprečevanja pranja denarja in financiranja terorizma obravnavati kot ključno za zagotovitev varnosti v svetu. Zaradi vedno bolj iznajdljivih načinov pranja denarja in financiranja terorizma je postalo preprečevanje teh dveh pojavov za banke zelo zahtevna naloga. Na srečo so države že zelo zgodaj spoznale, da teh težav ne bo mogoče rešiti na nacionalni ravni, zato so skupaj ustanovile mednarodne organe, ki skrbijo, da je soočenje z izzivi preprečevanja pranja denarja in financiranja terorizma kar se da usklajeno in poenoteno. Seveda so možnosti izboljšav na tem področju številne, a kot bo videno v nadaljevanju, je bilo doseženo že precejšnje poenotenje glede smernic, priporočil in zakonodaje, ki se uporablja za preventivo. Finančne institucije se tako srečujejo z obsežnimi zakonodajnimi zahtevami, ki jim jih predpisujejo regulatorji. Ker so tudi same pod pritiskom optimizacije stroškov, se vedno bolj opirajo na tehnične rešitve, ki jim omogočajo učinkovitejše zagotavljanje skladnosti poslovanja.

Magistrska naloga je namenjena kot pomoč bankam, da se bolj strukturirano in temeljito pripravijo ter izpeljejo proces izbire rešitve za preprečevanje pranja denarja in financiranja terorizma.

V prvem delu je predstavljena definicija pranja denarja in financiranja terorizma, analiza zgodovine in trenutnega stanja na področju preprečevanja pranja denarja in financiranja terorizma. Prav tako je v prvem delu podrobneje pojasnjen sam proces pranja denarja in financiranja terorizma. Temu delu sledi predstavitev napredka pri preprečevanju pranja denarja in financiranja terorizma, ki so ga države v okviru različnih mednarodnih organizacij dosegle na zakonodajnem področju, pri čemer je posebej izpostavljena ureditev preprečevanja pranja denarja in financiranja terorizma v Sloveniji.

V osrednjem, ključnem delu magistrske naloge, imenovanem izbira programske rešitve, so opredeljene zahteve iz Zakona o preprečevanju pranja denarja in financiranja terorizma, opisane rešitve za preprečevanje pranja denarja in financiranja terorizma in podrobneje prikazani ključni aspekti, ki jih je potrebno upoštevati pri izbiri rešitve za področje preprečevanja pranja denarja in financiranja terorizma. Bistvo osrednjega dela predstavlja prikaz kriterijev, ki so ključni pri izbiri rešitve za preprečevanje pranja denarja in financiranja terorizma in predlog matrike, s pomočjo katere se banke odločijo za izbiro najboljše rešitve. Sledijo sklep, ki povzame ključne ugotovitve magistrske naloge, literatura in viri ter priloge.

Cilj magistrskega dela je:

- pripraviti kriterije in matriko, s pomočjo katere bodo banke lahko izbirale rešitve za preprečevanje pranja denarja in financiranje terorizma.

V prvem delu magistrske naloge sem uporabil deskriptivno metodo raziskovanja, kjer sem predstavil definicijo, zgodovino in razvoj preprečevanja pranja denarja in trende, ki so relevantni za to področje v zadnjih letih. V nadaljevanju sem uporabil metodo analize in komparacije, kjer sem pripravil seznam členov iz osnutka novega Zakona o preprečevanju pranja denarja in financiranja terorizma (v nadaljevanju ZPPDFT) in izpostavil tiste, ki jim zadostimo z implementacijo ustrezne rešitve za preprečevanje pranja denarja in financiranja terorizma. V osrednjem delu magistrske naloge, kjer sem pripravil kriterije za izbiro rešitve za področje preprečevanja pranja denarja in financiranja terorizma, sem uporabil metodo poglobljenega intervjuja s strokovnjaki iz področja pranja denarja in financiranja terorizma.

1 PRANJE DENARJA IN FINANCIRANJE TERORIZMA

V večini držav predstavlja pranje denarja in financiranje terorizma velik izziv predvsem z vidika njegovega preprečevanja, odkrivanja in preganjanja. Vedno bolj izpopolnjene metode pranja denarja in financiranja terorizma samo še otežujejo odkrivanje teh dejanj. Pranje denarja je v osnovi preprost koncept. To je postopek, s katerim se prikriva izvor denarja, ki je bil pridobljen na način, ki se preganja po zakonu. Podobno preprosto se lahko opredeli tudi financiranje terorizma. Slednje je kakršnakoli finančna podpora terorizma ali tistih, ki vzpodbujajo, planirajo ali izvajajo teroristična dejanja (Schott, 2009, str. I-1).

1.1 Definicije pranja denarja

Po 2. členu Zakona o preprečevanju pranja denarja in financiranja terorizma (Ur.l. RS, št. 60/2007-ZPPDFT, v nadaljevanju ZPPDFT) je »pranje denarja katerokoli ravnanje, s katerim se prikriva izvor denarja ali drugega premoženja, pridobljenega s kaznivim dejanjem, in vključuje:

- zamenjavo ali kakršenkoli prenos denarja ali drugega premoženja, ki izvira iz kaznivega dejanja;
- skrivanje ali prikrivanje prave narave, izvora, nahajanja, gibanja, razpolaganja, lastništva ali pravic v zvezi z denarjem ali drugim premoženjem, ki izvira iz kaznivega dejanja«.

Po Direktivi Evropskega parlamenta in Sveta 2005/60/ES (Ur.l. EU, št. 309/15) je »pranje denarja naslednje naklepno ravnanje:

- preoblikovanje ali prenos premoženja, vedoč, da to premoženje izvira iz kaznivega dejanja ali udeležbe v takem dejanju, z namenom utaje ali prikrivanja nezakonitega

izvora premoženja ali pomoči osebi, ki je vpletena v storitev tega dejanja, da bi se izognila pravnim posledicam svojega dejanja;
- utaja ali prikrivanje prave narave, vira, kraja, razpolaganja ali pretoka premoženja ali pa pravic ali lastništva na premoženju, vedoč, da to premoženje izvira iz kaznivega dejanja ali udeležbe pri takem dejanju;
- pridobitev, lastništvo ali uporaba premoženja, vedoč v času prejema, da to premoženje izvira iz kaznivega dejanja ali udeležbe pri takem dejanju;
- udeležba, združevanje za izvrševanje, poskus storitve, pomoč, napeljevanje ter omogočanje in svetovanje pri storitvi kateregakoli dejanja iz prejšnjih točk.«

V pripravi je nov Zakon o preprečevanju pranja denarja in financiranja terorizma, ki pa same definicije pranja denarja ne spreminja (Predlog osnutka ZPPDFT, 2015).

1.2 Definicija financiranja terorizma

Zakon o preprečevanju pranja denarja in financiranja terorizma (Ur.l. RS, št. 60/2007-ZPPDFT) v 2. členu določa, da je:

»Financiranje terorizma je zagotavljanje ali zbiranje oziroma poskus zagotavljanja ali zbiranja denarja ali drugega premoženja zakonitega ali nezakonitega izvora, posredno ali neposredno, z namenom ali zavedajoč se, da bo v celoti ali delno uporabljeno za izvedbo terorističnega dejanja, ali da ga bo uporabil terorist oziroma teroristka (v nadaljevanju terorist) ali teroristična organizacija.«

V organizaciji Združeni narodi je bilo veliko truda vloženega v odkrivanje dejanj financiranja terorizma in mehanizmov, ki zagotavljajo finance za tovrstna dejanja. Schot (2009, str. I-4) ugotavlja, da so na podlagi lastnih ugotovitev z Mednarodno konvencijo o preprečevanju financiranja terorizma terorizem opredelili kot »vsakršno dejanje, ki povzroči smrt ali resne telesne poškodbe civilni osebi ali katerikoli drugi osebi, ki ne sodeluje aktivno v sovražnostih ali oboroženem konfliktu. Namen tega dejanja je zastraševanje prebivalstva oziroma prisila oblasti ali mednarodne organizacije v določeno dejanje«.

Tako kot definicija pranja denarja se tudi definicija financiranja terorizma ne spreminja v predlogu osnutka novega zakona o preprečevanju pranja denarja (Predlog osnutka ZPPDFT, 2015).

1.3 Povezava med pranjem denarja in financiranjem terorizma

Načini izvajanja pranja denarja so v veliki meri enaki kot načini prikrivanja virov in izvajanja financiranja terorizma. Za teroristične organizacije je pri tem ključno, da ti viri ostanejo prikriti, saj to teroristični organizaciji omogoča pridobitev sredstev tudi v prihodnje. Schott

(2009, str. I-5) pri tem ugotavlja, da je ključna razlika med pranjem denarja in financiranjem terorizma ta, da so sredstva pri slednjem lahko pridobljena na zakonit ali na nezakonit način. Posledično je zaradi tega treba sprejeti tudi posebne zakone, ki so namenjeni posebej financiranju terorizma.
Zelo pogosto se dogaja, da so aktivnosti in cilji pralcev denarja in financerjev terorizma prepleteni. Kriminalne organizacije vidijo koristi terorističnih skupin v njihovih sposobnostih izpeljave obsežnejših akcij, katerih cilj je uničenje in povzročanje kaosa. Medtem ko teroristične organizacije vrednost sodelovanja s kriminalnimi organizaciji vidijo v tem, da z njihovo pomočjo pridobijo dodatna sredstva za svoje delovanje. Pomemben je tudi podatek kako se področja, kjer delujejo teroristične organizacije, geografsko prekrivajo s področji, kjer so hkrati aktivne tudi kriminalne združbe, ki perejo denar. Takšen primer so Revolucionarne oborožene sile Kolumbije (znane tudi pod kratico FARC), katerih področje sovpada s področjem organiziranih kriminalnih združb, ki se ukvarjajo s pridelavo mamil in pranjem denarja. Drug primer so vojaki Al Kaide v Afganistanu, ki delujejo prav na območju, ki slovi po velikih količinah pridelanih opiatov. Kambodža, Čečenija, Šri Lanka in deli balkanskega polotoka pa so primer, kako se ideologija lahko zlorabi za namene razširjanja organiziranega kriminala in kako te organizirane družbe dajejo podporo terorističnim organizacijam (Thony, 2010).

Za banke je zelo pomembno, da razumejo tako povezave kot tudi razlike med pranjem denarja in financiranjem terorizma, hkrati pa je nujno, da vršijo vse kontrole in preverjanja za obe vrsti tveganj. Ker so določene kontrole za preprečevanje pranja denarja in preprečevanje financiranja terorizma zelo podobne ali celo enake, je priporočljivo, da se preverjanje teh kontrol izvaja znotraj iste rešitve z namenom, da se izogne podvajanju pravil v dveh rešitvah in posledično povečanju kompleksnosti na področju informacijske infrastrukture.

1.4 Zgodovina pranja denarja

Začetki pranja denarja segajo v leto 2000 pred našim štetjem. Že takrat so kitajski trgovci prikrivali svoje premoženje pred vladarji, saj so se bali, da jim bodo slednji pobrali ves dobiček, pridobljen s trgovino. Metode, ki so jih trgovci uporabljali, so podobne metodam, ki se uporabljajo tudi danes: zamenjava denarja v gibljiva sredstva, prenos denarja izven dosega rok vladarjev in trgovanje po napihnjenih cenah. Iz tega se je tudi razvila ideja območij, ki jim danes pravimo »offshore centri[1]«.V okviru slednjih se je razvila dejavnost utaje davkov ter postopki pranja denarja z namenom skriti, prenesti ali zamenjati premoženje, do katerega ima pravico nekdo drug. Zanimivo pri tem je, da se pomen pranja denarja skozi tisočletja ni spreminjal, drugačni so le mehanizmi, ki jih osebe, ki perejo denar, pri tem uporabljajo (Veselko, 2004, str. 4).

[1]Offshore center je finančni sistem, ki nerezidnečnim organizacijam nudi ugodno ali nerestriktivno finančno regulativo, dodatno pa k temu običajno še spada finančna tajnost in ugoden davčni režim z nizkimi davki.

Razlogi za pranje denarja v srednjem veku so bili posledica naukov cerkve, ki je odločila, da so obresti greh. S tem so prisilili posojilodajalce in trgovce, da so iznašli nove načine, kako pobirati visoke obresti in kako prikriti njihov originalni izvor. Pri tem so uporabili različne načine, kot so umetno zviševanje menjalnega tečaja, kjer so obresti predstavljale posebne premije za tveganje ali pa kot plačilo garanta pri zapoznelih plačilih. Prav tako so tudi že uporabljali navidezne posrednike (družbe, ki so služile za krinko in niso imele nobenih operativnih funkcij). Slednji so si denar izposodili in ga kasneje vrnili, obresti in posojila pa so v tem primeru predstavljale dobiček na vložen kapital (Veselko, 2004, str. 5).

Finančni kriminal se je v veliki meri razširil tudi v obdobju prohibicije v ZDA (zgodnje 20. stoletje). S prodajo alkohola, ki je bila takrat prepovedana, so združbe in posamezniki zaslužili velike vsote denarja, katerega izvor pa je bilo treba prikriti. Mayer Lansky, znan tudi kot pionir »offshore« bančništva, je spretno izkoristil prednosti storitev bank iz Švice s tem, ko je pri njih nalagal umazan denar za guvernerja Louisiane (Henryja Longa), v zameno pa mu je slednji izdal dovoljenja za odprtje igralnic v Ameriki. To metodo imenujemo metoda navidezna zadolževanja in je primer, kako s pomočjo kaznivih dejanj pridobljeni denar pretvoriti v »offshore« posojila. Dejstvo pa je tudi, da je takratna zakonodaja na področju pranja denarja bila zelo šibka oziroma je sploh ni bilo (Veselko, 2004, str. 5).

V 70. letih prejšnjega stoletja, tako Veselko (2004, str. 6), je tudi London, s svojo ureditvijo na področju finančnih institucij, privabil kar nekaj oseb, ki so se ukvarjali s pranjem denarja. Preko britanskih finančnih institucij je bilo namreč mogoče dostopati do »offshore« centrov, kot sta bila na Kanalski otoki (angl. *Channel Islands*) in Otok Man (angl. *Isle of Man*). Dodatno pa je k temu prispevala še značilna lastnost Angležev, njihova diskretnost in ugodna zakonodajna ureditev, ki bi morala biti precej bolj restriktivna. Veselko nadaljuje (prav tam), da je ravno ta nerestriktivnost bila zelo izražena pri enem izmed največjih škandalov povezanih s finančnim kriminalom − afera BCCI (angl. *The Bank of Credit and Commerce International*, v nadaljevanju BCCI). Cilj te banke je bil prikriti izvor denarja, ki je bil namenjen za financiranje vojne v Afganistanu. BCCI-banka je igrala vlogo vmesne postaje na poti med afganistanskimi mamili in ameriškim in britanskim orožjem. Banka je v svojem najdejavnejšem obdobju nakopičila ogromne količine denarja (23 milijard $), a je po koncu vojne v Afganistanu izgubila smisel svojega obstoja in zato so jo leta 1991 zaprli. Pri tem je zelo problematično to, da je večina sredstev te banke izginila in njihovo izginotje še danes ni pojasnjeno.

Drug primer, pri katerem je prav tako šlo za zlorabo velikih vsot denarja (1,4 milijarde $), je primer italijanske Banke Ambrosiano. V tej banki je do zlorabe prišlo, ker je banka izdala posojila »papirnati« družbi v Panami. Kot se je kasneje izkazalo, je vodja te družbe bil sam direktor Banke Ambrosiano, Robert Calvi, ki je s pomočjo nadškofa Marcinkusa, slednji je podal posojilne garancije za družbo v Panami, izpeljal prevaro. Prevara je takrat

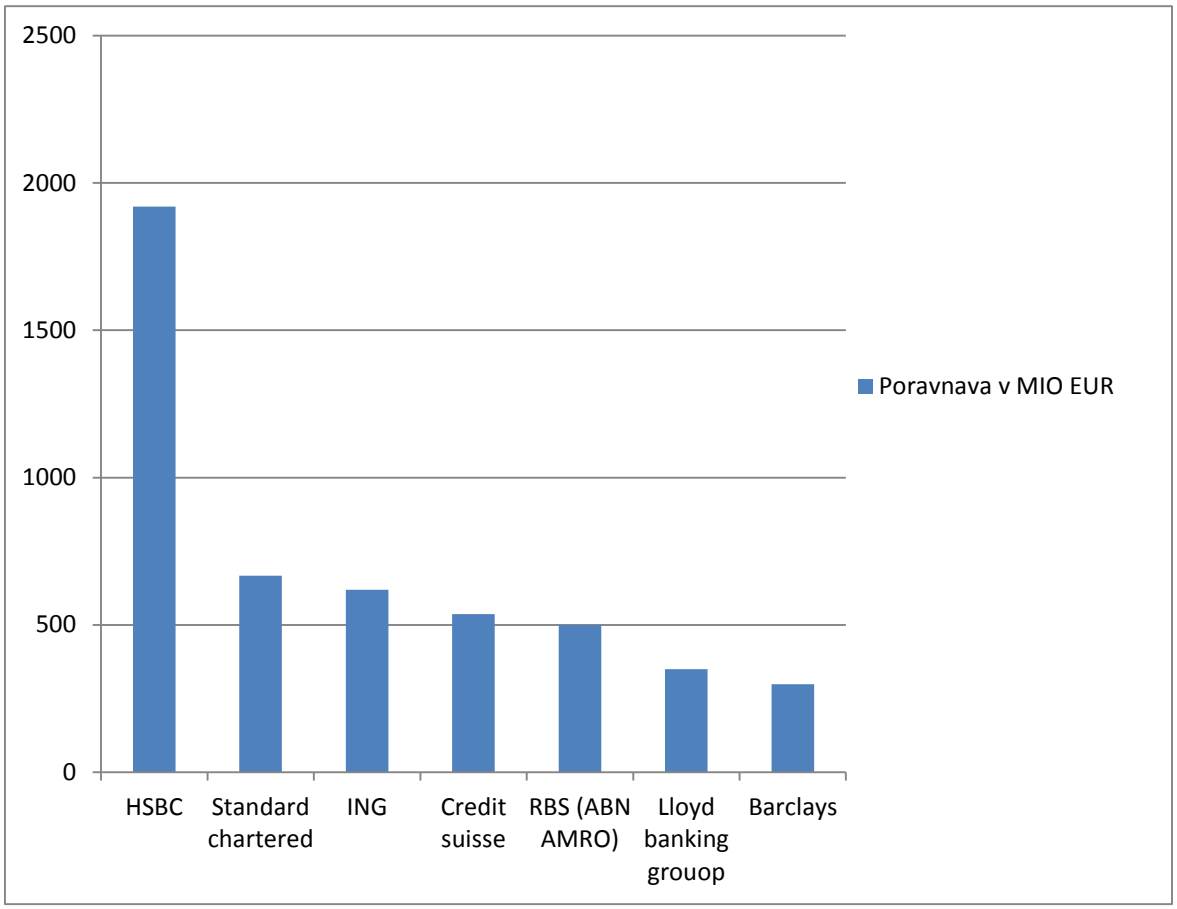
zamajala celoten italijanski finančni sektor. Ta prevara je dobila epilog, ko so Roberta Calvija, ki so ga zaradi njegovih poslov poznali tudi pod imenom »božji bančnik«, našli obešenega pod mostom Blackfriars v središču Londona (Kalb, 1982, str.1−2).

Dokaz, da je področje Pranja denarja in financiranja terorizma še kako aktualno, pa so tudi odkritja ob nedavnih terorističnih napadih. Pri tem je zelo zanimiv podatek, da so na primer za »Charli Hebdo«, napad v Parizu, storilci potrebovali zelo omejeno vsoto denarja za izvedbo. Ker nihče izmed storilcev ni imel redne službe, bi bilo na primer tudi možno, da so se financirali na naslednji način: 6000 EUR potrošniškega kredita, pridobljenega s ponarejenimi dokumenti, prodajo rabljenega avtomobila in preprodajo ponarejenih, ukradenih izdelkov. Da gre v primeru terorističnih organizacij lahko tudi za zelo dobro organizirane družbe, dokazujejo dokumenti, najdeni s strani ameriške vojske pri predhodnici ISIL-a (Iraška veja Al Kaide), saj so slednji uporabljali napredene prakse za upravljanje s prihodki in stroški, ki so bili pripravljeni v skladu s standardiziranimi računovodskimi standardi. Ker bančni sektor zagotavlja najzanesljivejši in najučinkovitejši način mednarodnega prenosa sredstev, je tudi zelo izpostavljen tveganjem za pranje denarja in financiranje terorizma. To ugotavlja tudi poročilo o tihotapljenju drog v Afganistanu (2014), kjer se je za prenos sredstev uporabil bančni sistem. Posebej so bili pri tem izpostavljeni računi nevladnih organizacij, ki so dostavljali denar teroristični celicam (Financial Action Task Force, 2016).

Pri obravnavanju financiranja terorizma je treba razumeti, da so prav finance tiste, ki omogočajo terorističnim organizacijam dosego njihovih ciljev in izvedbo različnih operacij. Več faktorjev je pripomoglo k tako hitri razširitvi Islamske države (angl. *Islamic State of Iraq and the Levant - ISIL*), ampak zagotovo je bil eden ključnih prav zasedba ozemlja, bogatega z nafto, ki jim omogoča dober in zanesljiv vir financiranja (Association of Certified Anti-Money Laundering Specialists, 2015).

Kot je razvidno iz dogodkov zadnjih let, se pomembnost preprečevanja pranja denarja in financiranja terorizma krepi. Kazalnik tega so tudi kazni, ki so jih banke pripravljene plačati v primeru, ko njihovo delovanje ni skladno s predpisi. Pri tem je treba izpostaviti, da te kazni izvajajo ameriški regulatorji, ki imajo zaradi vpliva na trgovanje z valuto dolarji, sredstva, da dosežejo prilagoditev bank pravilom za preprečevanje pranje denarja in financiranje terorizma. Primeri največjih poravnav s tega področja so prikazani v Sliki 1.

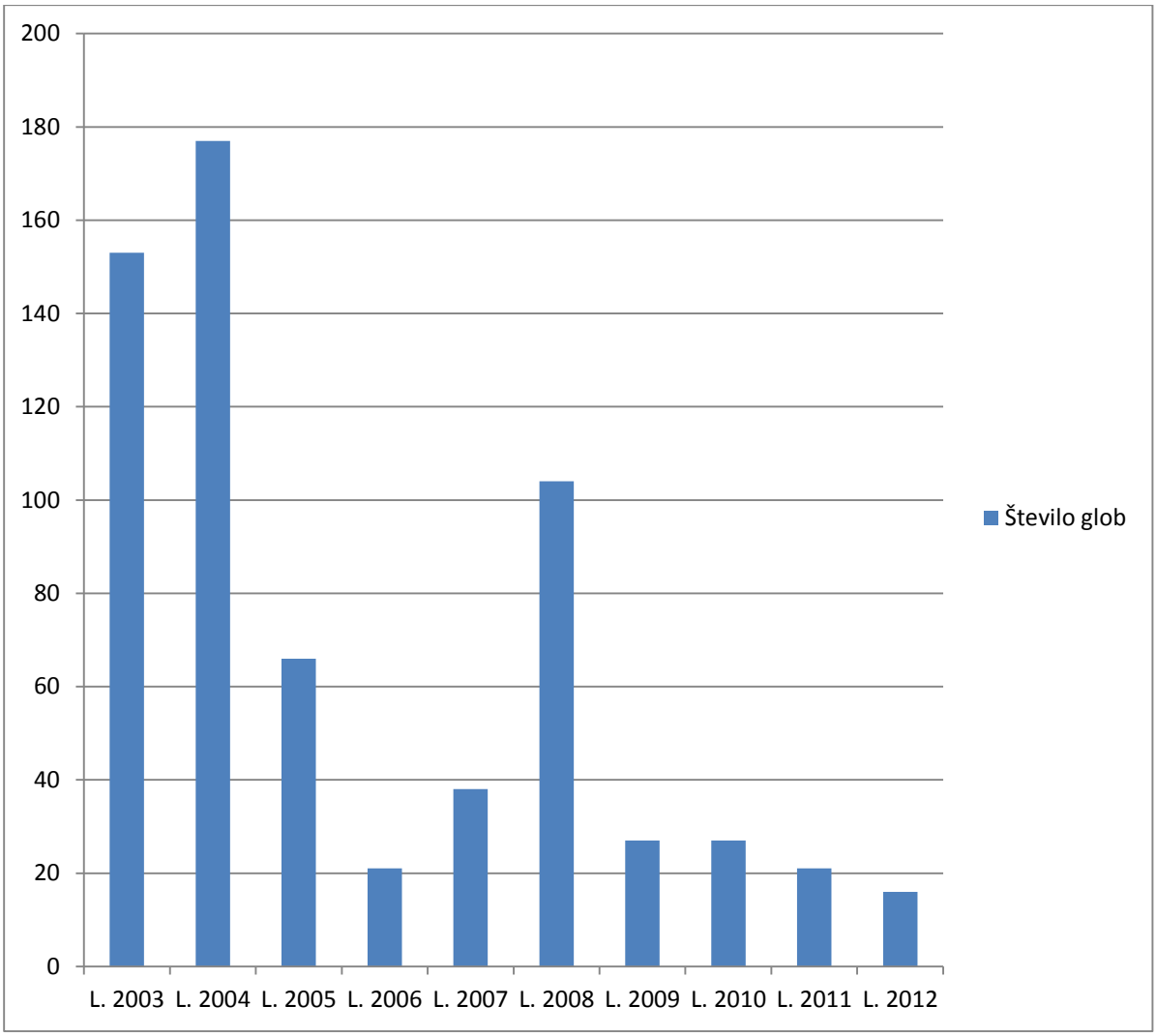
Slika 1: Največje poravnave z ameriškimi oblastmi zaradi pranja denarja



Vir: Money – laundering settlements, 2012.

Implementacija rešitev za preprečevanje pranja denarja in financiranje terorizma predstavlja za banke velik strošek. Po drugi strani lahko imajo precejšnje prihodke iz naslova sredstev, ki so pridobljeni s predhodnim kaznivim dejanjem. V zadnjih treh letih je bila večina največjih bank kaznovana za aktivnosti, povezane s kriminalnimi dejanji pranja denarja. Ravno zaradi tega vidimo zelo velike investicije v rešitve za preprečevanje pranja denarja. Te velike banke najemajo najboljše strokovnjake na svetu, da jim pomagajo pridobiti najboljše rešitve, ki so trenutno na trgu. Trend, ki je opazen kot posledica tako velikih glob, je ukinjanje sodelovanja s celotnimi segmenti strank v določenih državah, s čimer pa se te stranke samo preusmeri v gotovinsko poslovanje, namesto da bi se jih identificiralo kot kršitelje PPDFT pravil (Lewis, 2016). V obdobju povečevanja pritiskov s strani zakonodaje in nadaljevanja prizadevanj, da bi se poenotila pravila za preprečevanja pranja denarja in financiranja za vse države, se banke srečujejo z vedno večjimi izzivi kako vzpostaviti ustrezne kontrole in potem dolgoročno zagotavljati skladnost s pravili na tem področju. Pri tem je zanimivo, da je samo število glob v zadnjih letih upadlo (Slika 2), a se je hkrati višina glob za vsako posamezno kršitev izredno povečala. V tem se vidi velika odločenost zakonodajalcev, da preprečijo kršitve pravil in izvajajo pritisk na osebe, odgovorne za skladnost v bankah.

Slika 2: Gibanje količine izdanih glob v letih 2003–2012



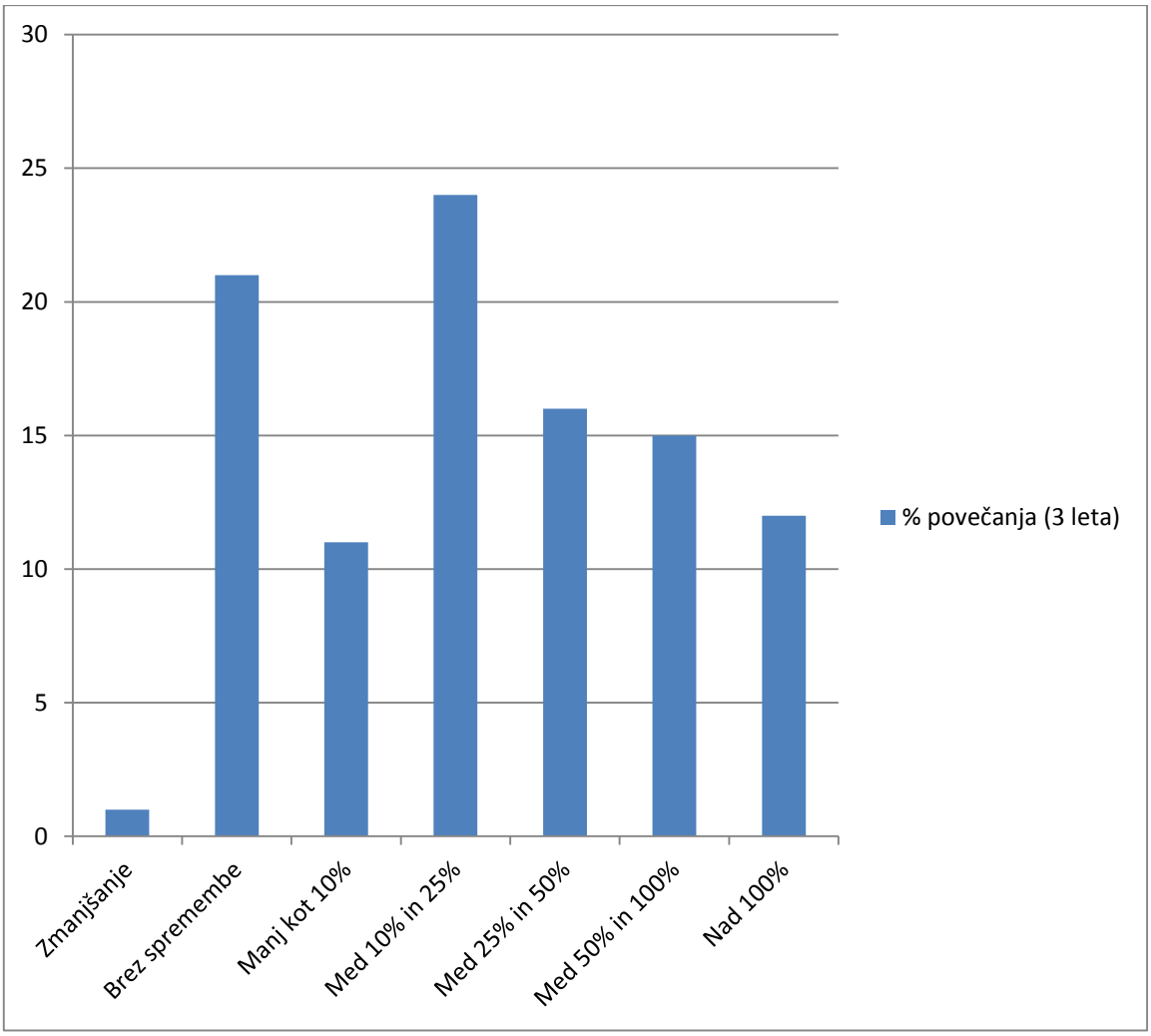
Vir: Acuity, Trend in Anti-Money Laundering (AML) compliance, b.l..

Kazni pa niso edino, kar banke potiska k izpolnjevanju pravil. Vedno bolj je v ospredju tudi potencialna izguba dobrega imena, kar je predvsem v finančnem svetu ključnega pomena. Primer ukrepanja na podlagi tega vzroka je bil nedavno izkazan na primeru tako imenovane »Vatikanske banke«, kjer so se zaradi primerov kriminalnih dejanj odločili zamenjati celotno višje vodstvo družbe (Massimo, 2013).

Dejstvo je, da so se banke na ta dejanja tudi odzvale, to je namreč razvidno v rasti investicij (glej graf 3 spodaj), ki jih banke in druge finančne institucije namenjajo za ta področja.

Globe in vedno strožje zakonodajne zahteve zahtevajo od bank vzpostavitev rešitev, ki jim omogočajo uspešno spopadanje z novimi grožnjami. Zaradi tega se tudi količina investicij v področje preprečevanja pranja denarja in financiranja terorizma (v nadaljevanju PPDFT) povečuje (Slika 3).

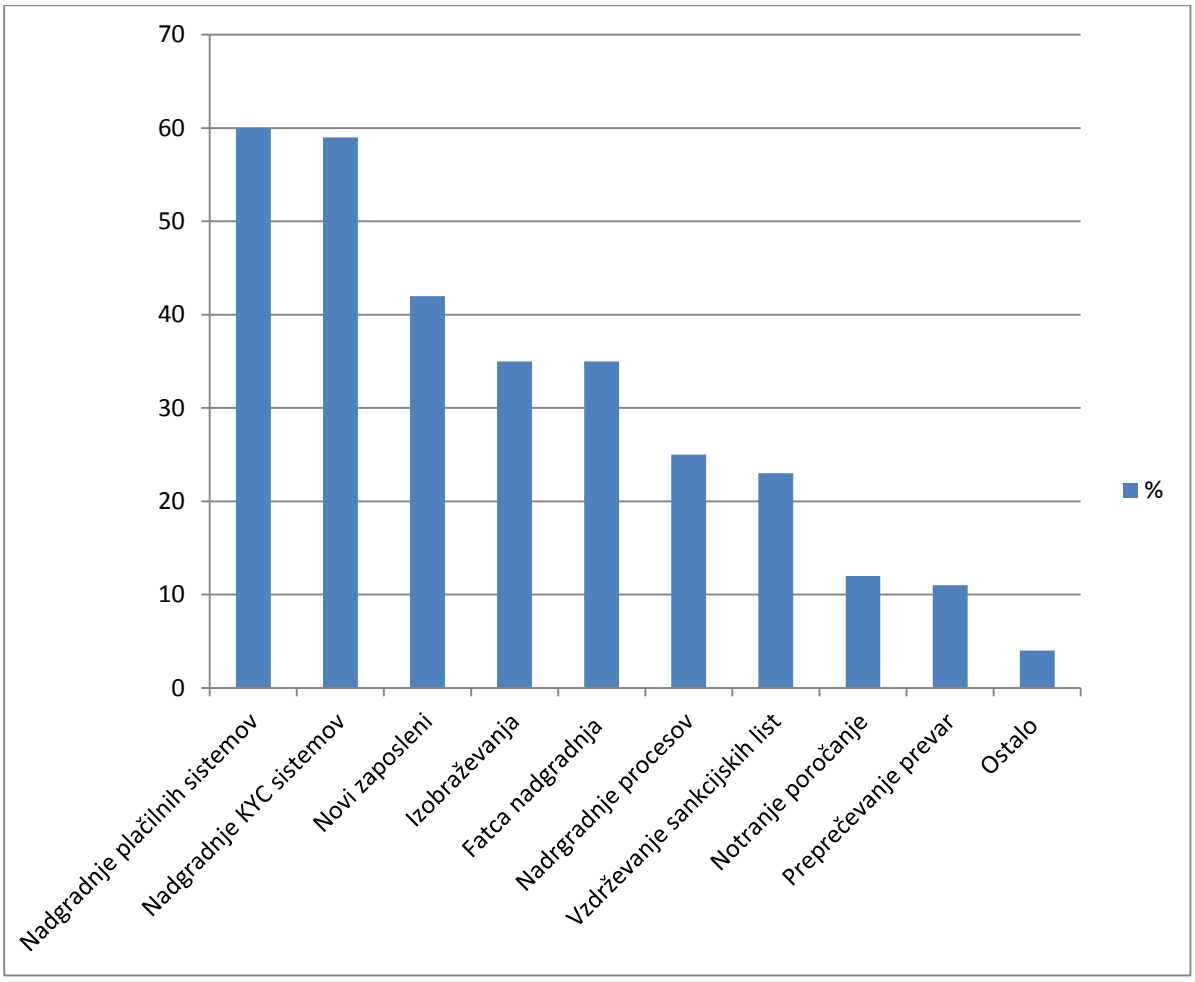
Slika 3: Prikaz povečanja investicij v PPDFT-področje v preteklih treh letih



Vir: KPMG, Information technology – tool for addressing you AML risks, b.l..

Glede na trend povečevanja investicij je ključno tudi, zakaj so sredstva teh investicij v nadaljevanju porabljena (Slika 4). V svoji raziskavi (KPMG, 2016) je podjetje KPGM na podlagi odgovorov več kot 300 strokovnjakov s področja PPDFT ugotovilo, da se je največ vlagalo v plačilne sisteme (60 % vprašanih). Zelo pomembne z vidika porabe investicij (59 % vprašanih) so tudi nadgradnje rešitev za poznavanje stranke (angl. *Know your customer*, v nadaljevanju KYC). Takoj za tem pa sledijo investicije v nove zaposlene (42 % vprašanih) in izobraževanje (35 % vprašanih), saj postaja vedno bolj očitno, da brez visoko usposobljenih strokovnjakov tako kompleksnega področja ni mogoče pokrivati. Največjih pet področij zaključuje vzpostavitev rešitve za poročanje Zakona o spoštovanju davčnih predpisov v zvezi z računi v tujini (angl. *Foreign Account Tax Compliance Act*, v nadaljevanju FATCA), ki je posledica Sporazuma o spoštovanju davčnih predpisov v zvezi z računi v tujini, katerega namen je preprečevanje in odkrivanje davčnih utaj ameriških davčnih zavezancev, ki neposredno ali posredno investirajo zunaj Združenih držav Amerike (v nadaljevanju ZDA), preko neameriških finančnih institucij.

Slika 4: Največje investicije na področju pranja denarja in financiranja terorizma



Vir: KPMG, Information technology – tool for addressing you AML risks, b.l..

1.5 Trendi pranja denarja

Tradicionalne metode pranja denarja so se osredotočale na področje gotovinskega poslovanja. Te metode ostajajo aktualne tudi danes. Poleg tega pa se danes pojavljajo nove in inovativne metode, ki izkoriščajo slabosti v finančnih sistemih. Nepremičnine, posojila in različne oblike trgovanja, ostajajo prednostne metode, ki jih pralci denarja uporabljajo. Povečala se je tudi uporaba kreditnih kartic s strani strank »offshore« bank in pričakuje se, da bodo pralci denarja izkoriščali ranljivosti novih tehnologij, kot so na primer elektronski denar, prodaja preko svetovnega spleta in kockanje (Organisation for Economic cooperation and development, 2015, v nadaljevanju OECD).

Z zaostrovanjem zakonodaje na področju pranja denarja in financiranja terorizma so se razvijali in spreminjali tudi trendi pranja denarja, ki so navedeni v nadaljevanju (povzeto po Šeme Hočevar, 2007, str. 31−36):

- **Vključevanje »poklicnih pralcev denarja«**

Pri tej metodi gre za uporabo poklicnih finančnih posrednikov s strani kriminalnih organizacij. Na ta način se povečuje učinkovitost pranja denarja, saj so ti posamezniki posebej izurjeni in izobraženi. Pri tem gre posebej omeniti odvetnike, notarje in računovodje, ki so vključeni kot zastopniki v primeru ustanavljanja podjetij.

- **Fizični prenosi gotovine**

To je še vedno ena izmed najpogostejših metod, kljub težavam, ki jih povzročata teža in količina denarja. Na našem območju se največkrat uporablja klasičen način (v osebni prtljagi, torbah, avtomobilih).

- **Uporaba gospodarstva in prostih trgovinskih con**

Pogost primer je tudi uporaba navideznih računov za določene izdelke ali storitve ali pa nerealno višanje cen določenih izdelkov. V tem primeru se kriminalci povežejo z uvoznimi podjetji in nastopijo kot posredniki storitve ter plačajo izvoznikom v tujino v tuji valuti. Slednji jim potem vrnejo denar v domači valuti, a po tečaju, ki je ugodnejši od veljavnega menjalniškega tečaja.

- **Uporaba nebančnih finančnih institucij**

Pri tej metodi se uporabi menjalnice, agencije za izplačevanje potovalnih čekov, zavarovalnice, borzne posrednike, prireditelje dražb, zlatarjev, draguljarn ali igralnic. Tudi v prihodnosti se predvideva, da bo velik del pranja denarja potekal preko teh organizacij.

- **Uporaba podjetij, katerih poslovanje temelji na gotovini**

Tukaj izstopajo predvsem hoteli, podjetja za hitro dostavo hrane, igralnice in tudi loterija. Predvsem pri igralnicah lahko pralci denarja z dogovorjenim večjim dobitkom operejo velike količine denarja. Enako velja za loterijske srečke, kjer se je loterijska srečka kupila pa bistveno višji ceni, kot je bila nagrada. Kupec je tako za srečke plačal z umazanim denarjem in se nato na okencu za izplačilo prikazal kot legitimni lastnik.

- **Uporaba elektronskih prenosov**

Z vedno bolj razširjeno uporabo elektronskih poti v bančništvu so tudi pralci denarja začeli uporabljati te storitve. Banke in borzno-posredniške hiše, ki delujejo 24 ur dnevno, so kot nalašč za pralce denarja. Kljub mnogim predpisom in določbam, ki predpisujejo obvezno podajanje podatkov o pošiljatelju in prejemniku denarja, se vedno znova pojavljajo primeri, ko je pošiljatelj neznan ali pa podatki o njem niso popolni.

- **Izkoriščanje offshore bančništva**

Veliko so k slabitvi sledenju pralcem denarja prinesli tudi »offshore« bančni centri. Tukaj je očitna tudi napaka centralnih bank, ki niso opazile, da bodo z dovoljenjem matičnim bankam, da le-te ustanovijo »offshore« podružnice, izgubile nadzor nad njimi.

- **Uporaba novih finančnih instrumentov**

Zelo hiter razvoj novih bančnih instrumentov otežuje pravočasno vzpostavitev pravnih okvirjev, ki bi ustrezno zaščitili tako ponudnike kot tudi uporabnike teh storitev in zagotovili transparentnost poslovanja.

- **Uporaba nove bančne prakse**

Razvoj tehnologije omogoča stranki hitro in prilagodljivo izvajanje bančnih storitev. Spletno bančništvo občutno zmanjša možnost neposredne identifikacije stranke pri opravljanju transakcij. Ključna težava tukaj so banke, ki nudijo svoje storitve brez neposredne identifikacije stranke ob odprtju računa.

- **Vključevanje držav v tranziciji**

Trend v pranju denarja je tudi vključevanje držav v tranziciji. Tukaj gre v veliki meri za države srednje in vzhodne Evrope, kjer se zaključujejo ali pa so bili nedavno zaključeni postopki privatizacije, kjer je želja po neposrednih tujih naložbah velika in kjer je kriminal prisoten v veliko finančnih institucijah.

1.6 Obseg težav zaradi pranja denarja in financiranja terorizma

Obseg težav zaradi pranja denarja in financiranja terorizma je težko oceniti, saj sta to prikrita pojava in ju je zato težko prikazati v kakršnihkoli statističnih analizah. Dodatno oceno otežuje tudi dejstvo, da je večina teh dejanj izvedena v različnih državah. Mednarodni denarni sklad je ocenil, da bi skupni znesek opranih sredstev v svetu lahko znašal med 2 % in 5 % svetovnega bruto proizvoda. Ne glede na različnost teh ocen pa v svetu vlada splošno strinjanje, da tako pranje denarja kot tudi financiranje terorizma predstavljata zelo resno težavo, ki ji mora vsaka država posvečati posebno pozornost (Schott, 2009, str. 1−5).

Glede na oceno mednarodnega denarnega sklada bi lahko potencialna skupna vsota opranega denarja znašala nekje 2 trilijona ameriških dolarjev. Zelo problematično je, da po podatkih Urada Združenih narodov za droge in kriminal (UNODC), le okoli 1% tega denarja zasežejo oblasti v okviru ukrepov za preprečevanje pranja denarja. Zaradi povečanega števila terorističnih napadov in velike škode, ki jih le ti povzročijo, se je veliko držav pričelo intenzivno ukvarjati s področjem preprečevanja teh tveganj. Pričakuje se, da bodo državni organi odgovorni za področje preprečevanja pranja denarja in financiranja terorizma pričeli strogo spremljati in kaznovati organizacije, ki ne bodo skladne z regulativami na tem področju. Posledice teh dodatnih kontrol in razširjenih zahtev s strani zakonodajalcev, bodo neizogibno vodile v rast stroškov, ki jih morajo banke namenjati za to področje. Po podatkih podjetja Wealthinsight se pričakuje, da bo strošek porabljenih sredstev za preprečevanje pranja denarja, globalno gledano, v letu 2017 dosegel številko 8 milijard ameriških dolarjev, kar pomeni približno 9% letno rast (PWC, 2016).

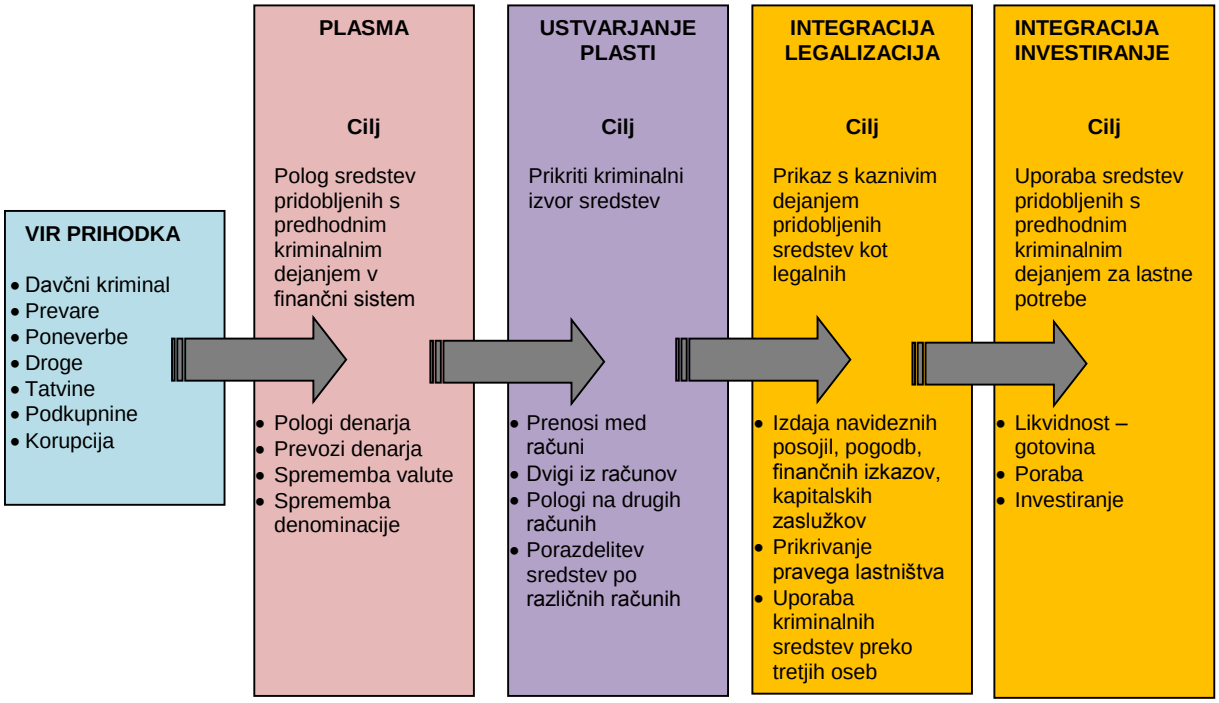
Čeprav v Sloveniji zelo velikih in odmevnih primerov pranja denarja ali financiranja terorizma nismo imeli, se banke še predobro zavedajo, da so del mednarodnega okolja in kot take zelo izpostavljene tem tveganjem. Ker so banke odvisne od zaupanja ljudi, ki pri njih hranijo denar, se bodo tudi v našem bančnem sektorju nadaljevala vlaganja v nove in učinkovitejše rešitve za preprečevanje pranja denarja in financiranja terorizma.

1.7 Proces pranja denarja in financiranja terorizma

Cilj pralcev denarja je prikriti izvor denarja in tako imenovani umazani denar oprati z namenom, da bo oteženo ali onemogočeno izslediti prvotni izvor tega denarja in bo kasneje lahko uporabljen brez, da bo vzbudil kakršenkoli sum. Ne glede na to, ali je bilo predhodno kriminalno dejanje povezano z davčno prevaro, prepovedanimi drogami, nezakonito prodajo orožja, korupcijo itd., se za pranje denarja uporabi proces, ki ga razdelimo v tri faze: plasma, ustvarjanje plasti in integracija. Faza integracije se lahko razdeli še na podfazi: legalizacija in investiranje (Office of Foreign assets Control, 2015).

Proces pranja denarja poteka od vira prihodka, ki je najpogosteje posledica predhodnega kaznivega dejanja, do plasmaja, kjer se poskuša sredstva položiti v finančni sistem, znotraj katerega se izvaja aktivnosti iz naslova prikrivanja izvora sredstev z ustvarjanjem različnih plasti. Proces se nato nadaljuje s fazo integracije – legalizacije, kjer se sredstva, pridobljena s kaznivim dejanjem, poskušajo prikazati kot legalna. Po zaključku faze integracije – legalizacije pa se v okviru faze integracija investiranje začne porabljati sredstva (Slika 5).

Slika 5: Podroben pregled procesa pranja denarja po OECD



Vir: Office of Foreign assets Control. Money Laundering Awareness handbook for Tax Examiners and Tax Auditors, 2015, str. 10.

1.7.1 Plasma

Cilj te faze je položiti sredstva, pridobljena s predhodnim kaznivim dejanjem na bančni račun doma ali v tujini. Za ta namen se lahko gotovino tudi zamenja za zlato, diamante ali čeke. Lahko se jih tudi zamenja v druge valute in se jih razdeli v manjše zneske, da se omogoči lažji transport. Prenosi teh sredstev se lahko izvajajo z avtomobili, letali ali pa preko bančnega sistema. Za vse te aktivnosti lahko pralci denarja uporabljajo pomoč tretjih oseb, tako fizičnih kot tudi podjetij (Office of Foreign assets Control, 2015, str. 13).

1.7.2 Ustvarjanje plasti

Pri fazi ustvarjanja plasti je glavni cilj prikrivanje sledi za izvorom denarja. Slednje se največkrat izvaja tako, da se sredstva preusmerjajo iz banke na banko v različnih državah, med različnimi posamezniki in podjetji in z različnimi zneski, vse to pa z namenom otežiti oziroma onemogočiti sledljivost. V tej fazi se sredstva velikokrat prenesejo v države z zelo strogimi režimi za varovanje osebnih podatkov ali pa se uporabi podjetja iz »offshore« bank kot lastnike računov (Office of Foreign assets Control, 2015, str. 13).

1.7.3 Integracija

Fazo integracije lahko delimo na dve podfazi: legalizacijo in investiranje.

- ***Legalizacija***

Cilj te faze je, da se sredstva, pridobljena s predhodnim kaznivim dejanjem, prikaže kot legalna. To se lahko prikaže na naslednje načine:

1. Prikaz lastnega poslovanja (poneverba prikaza virov prihodkov, zaslužki na kapitalskih trgih in / ali s posojili.
2. Prikrivanje lastništva.
3. Uporaba teh sredstev v transakcijah s tretjimi osebami.

V tej fazi pralec denarja s pomočjo poneverb (računov, pogodb …) prikaže sredstva, ki so v njegovi lasti kot zakonita. Običajne metode, ki jih uporabi, da prikaže ta sredstva kot legalna, so:

1. Poneverba preko posojil (fiktivna posojila, nerealne obrestne mere).
2. Poneverba preko neto vrednosti premoženje (nakup in prodaja nepremičnin, sredstva pridobljena z igrami na srečo, loterijski dobitki, dedovanje).
3. Prikrivanje lastništva (povezave z offshore podjetji ali sorodniki kot zakonitimi lastniki).
4. Manipulacije s cenami (računi s prevelikimi ali premajhnimi cenami).

5. Poneverbe prikazov prihodkov, na katerih se združuje zakonito in nezakonito pridobljena sredstva.

- ***Investiranje***

Cilj te faze je uporaba sredstev, pridobljenih s predhodnim kriminalnim dejanjem za lastno korist. Gotovina ali elektronski denar sta lahko uporabljena za:

1. Hranjene (denar v nogavici).
2. Porabo (dnevna poraba, nakit, avtomobili, jahte, umetniška dela …).
3. Investicije (depoziti, nepremičnine, delnice, financiranje legalnih in nelegalnih podjetij …).

V tej fazi se pojavi razkazovanje bogastva oziroma bogatega stila življenja s strani pralcev denarja z nabavo luksuznih stvari: jahte, nakit … Pralci denarja si prizadevajo oprati denar zato, da si lahko potem kupijo te dobrine, brez da bi jih skrbelo, da bodo zaradi tega kazensko preganjani (Office of Foreign assets Control, 2015, str. 13–14).

2 UREDITEV PREPREČEVANJA PRANJA DENARJA IN FINANCIRANJA TERORIZMA V SVETU

Skladnost držav s pravili za preprečevanje pranja denarja in financiranja terorizma igra zelo veliko vlogo pri integriteti svetovnega finančnega sistema. Ker se pranje denarja in financiranje terorizma pojavlja v različnih oblikah in na različnih ekonomskih področjih, so standardi, ki urejajo to področje, precej obsežni in kompleksni. Pri tem je pomembno izpostaviti, da predvsem za razvite države velja, da so v večini skladne s standardi na tem področju in da je za doseganje skladnosti nujna ustrezno urejena nacionalna zakonodaja. (IMF Compliance with the AML/CFT international standards, 2011, str. 6−7).

V tem poglavju so predstavljene različne mednarodne organizacije in pomembnejši zakonski predpisi, ki so bili izdani s strani teh organizacij, ki govorijo o preprečevanju pranja denarja in financiranju terorizma.

2.1 Združeni narodi

Mednarodno sodelovanje z namenom preprečevanja pranja denarja in financiranja terorizma je odsev strategije mnogih držav, ki so se sporazumele, da je to sodelovanje nujno potrebno, če želijo omejiti ekonomsko moč kriminalnih in terorističnih organizacij ter posameznikov, ki s pomočjo kaznivih dejanj pridejo do sredstev in le te kasneje skozi svoje aktivnosti operejo za nadaljnjo rabo. Zelo pomembno pri tem je, da s temi ukrepi zaščitijo tudi lastno ekonomijo (United Nations office on Drug and Crime, 2016).
Najpomembnejše konvencije Združenih narodov za področje PPDFT so bile:

- Konvencija združenih narodov zoper nezakonit promet mamil in psihotropnih snovi iz leta 1988.

Konvencija predstavlja temeljni pravni vir, ki prvič opredeli pranje denarja kot kriminalno dejavnost. Najpomembnejši element te konvencije je bil uvedba obveznosti za vse države podpisnice, da inkriminirajo kazniva dejanja, povezana s trgovanjem z mamili. Konvencija vsebuje še določila, ki urejajo preprečevanje, odkrivanje in zatiranje pranja denarja. Sporazum predvideva tudi obvezno sodelovanje med državami ter ukinja bančno tajnost v primerih preiskave (Šeme Hočevar, 2007, str. 45−47). H konvenciji je pristopilo 189 držav, med njimi tudi Slovenija, ki jo je med svoje predpise sprejela po osamosvojitvi kot naslednica Socialistične federativne republike Jugoslavije (United Nations Treaty Collection, 1988).

- Konvencija ZN proti mednarodnemu organiziranemu kriminalu (2003) in Konvencija ZN proti korupciji (2005).

Konvenciji sta bili sprejeti septembra 2003 in decembra 2005. Obe konvenciji širita obseg kaznivih dejanj, ki spadajo na področje pranja denarja in sedaj poleg kaznivega dejanja tihotapljenja drog vsebujejo predhodna kazniva dejanja v širšem smislu ter tudi huda kazniva dejanja. Poleg tega ti konvenciji krepita še sodelovanje med državami in zahtevata vzpostavitev Enot za finančni nadzor (angl. *Financial intelligence units*, v nadaljevanju FIU).

- Mednarodna konvencija o zatiranju financiranja terorizma (2002).

Mednarodna konvencija o zatiranju financiranja terorizma je stopila v veljavo leta 2002. Od članic zahteva vzpostavitev ukrepov za zaščito njihovega finančnega sistema pred zlorabami oseb ali organizacij, vpletenih v teroristične aktivnosti (United Nations office on Drug and Crime, 2015).

- Globalna strategija OZN za boj proti terorizmu (2006).

Poleg zgoraj naštetih konvencij je bila leta 2006 sprejeta še Globalna strategija OZN za boj proti terorizmu. Resolucija in akcijski načrt, ki sta del te strategije, predstavljata instrument, na podlagi katerega bodo države okrepile aktivnosti za boj proti terorizmu tako na nacionalni, regionalni kot tudi mednarodni ravni (United Nations office on Drug and Crime, 2015).

2.2 Konvencije Sveta Evrope

- Konvencija Sveta Evrope št. 141.

Konvencijo Sveta Evrope o pranju, odkrivanju, zasegu in zaplembi premoženjske koristi, pridobljene s kaznivim dejanjem, je Slovenija ratificirala 23. aprila 1998. Ta konvencija predstavlja enega izmed temeljnih mednarodnih aktov na področju pranja denarja in vključuje naslednje (Council of Europe, b.l.a). Konvencija je vzpostavila podlago za mednarodno sodelovanje in vzajemno pomoč. Razširila je definicijo pranja denarja, ki je

sedaj opredeljena kot premoženjska korist, ki izvira iz vseh oblik hudega kriminala in ne le iz prodaje prepovedanih mamil (terorizem, organiziran kriminal, izsiljevanje, ugrabitev, gospodarsko prevaro in drugo).

- Konvencija Sveta Evrope št. 198.

Svet Evrope je sprejel novo konvencijo, in sicer Konvencijo Sveta Evrope št. 198, ki jo je Slovenija ratificirala 26. aprila 2010 (Council of Europe. b.l.b). Konvencija 198 je prevzela večino standardov skupine Egmont, določbe o financiranju terorizma in uvedla obrnjeno dokazno breme v zvezi s hudimi kaznivimi dejanji. Zamrznitve, zaseg in odvzem je razširila tudi na premoženje, v katero je bila premoženjska korist spremenjena, in na zakonito pridobljeno premoženje, če je bilo to pomešano z »umazanim« premoženjem, ter na dobiček ali na drugo korist, ki izhaja iz »umazanega« premoženja. Prav tako je prevzela tudi velik del priporočil finančne delovne skupine o pranju denarja (angl. *Financial Action Task Force,* v nadaljevanju FATF[2]) iz leta 2003 (Šeme Hočevar, 2007, str. 75−78). Avtorica Šeme Hočevar (2007, str. 75−78) še izpostavlja, da Konvencija št. 198 uvaja tudi odgovornost pravnih oseb za kaznivo dejanje pranja denarja in je prvi mednarodni akt z zavezujočimi določbami, ki ureja definicijo, nekatera pooblastila in mednarodno sodelovanje uradov za preprečevanje pranja denarja ter vsebuje določbe o preventivnih ukrepih. Konvencija posega tudi v delovanje nadzornih organov in zahteva vzpostavitev regulatornega in nadzornega sistema za preprečevanje pranje denarja. Predpisuje tudi obvezno ustanovitev uradov (FIU – Financial intelligence unit) za preprečevanje pranja denarja in financiranja terorizma ter zagotovitev zadostnih finančnih in tehničnih sredstev, kadrov in dostopa do finančnih, upravnih in policijskih podatkov, ki jih urad potrebuje za izvrševanje svojih nalog. Šeme Hočevarjeva še ugotavlja (prav tam), da je Konvencija št. 198 prinesla precej novosti, hkrati pa je mehka priporočila skupine FATF in pravila skupine Egmont preoblikovala v zavezujočo obliko.

- Konvencija Sveta Evrope o preprečevanju terorizma številka 196 in Protokol h konvenciji številka 217 o preprečevanju terorizma.

Na temo preprečevanja terorističnih groženj je svet Evrope sprejel dva dokumenta, in sicer Konvencijo Sveta Evrope o preprečevanju terorizma številka 196 in Dodatni protokol h konvenciji o preprečevanju terorizma, Konvencijo številka 217. Cilj sprejetja Konvencije je bil krepitev učinkovitosti obstoječih mednarodnih predpisov s področja preprečevanja terorizma, medtem ko Protokol dodatno razširja definicijo kaznivih dejanj s področja terorizma, ki bodo vključevale tudi sodelovanje v skupinah, ki so na seznamu terorističnih organizacij ali potovanja v tujino z namenom udeležbe na terorističnih treningih. Dodatno Protokol zahteva 24-urno nacionalno kontaktno točko, ki bo na voljo za hitro izmenjavo informacij (Šeme Hočevar, 2007, str. 75−78).

[2] Več informacij o FATF priporočilih je navedenih v poglavju 2.4. FATF (Projektna skupina za finančno ukrepanje).

2.3 Evropska unija

Evropska unija je že veliko let zagovornica večjega medsebojnega sodelovanja med državami z namenom skupnega boja proti kriminalu. Njena prizadevanja pa se odražajo v uredbah, ki jih sprejema.

- Direktiva Sveta št. 91/308/EGS (1991)

Prvo direktivo št. 91/308/EGS je Evropska unija sprejela v letu 1991. Cilje te direktive je bil preprečevanje uporabe finančnega sistema za namene pranja denarja. Primarni vzrok za to direktivo je bila skrb, da bo finančni sistem uporabljen za pranje denarja. S to direktivo so bili vzpostavljeni ključni preventivni mehanizmi, kot so identifikacija strank, hranjenje dokumentacije o strankah in njihovi aktivnosti in vzpostavitev metod za poročanje sumljivih transakcij (Anti Money laundering Forum, b.l.).

- Direktiva evropskega parlamenta in Sveta št. 2001/97/ES (2001).

Direktivo št. 91/308/EGS iz leta 1991 je leta 2001 nasledila direktiva št. 2001/97/ES, ki je odpravila pomanjkljivosti prve direktive. Ključne spremembe so zajemale opredelitev in razširitev zavezancev, ki so dolžni poročati uradu sumljive transakcije ter razširitev kaznivega dejanja pranja denarja, ki je po tej direktivi zajemala vsa huda kazniva dejanja in ne več samo trgovanja z mamili (Anti Money laundering Forum, b.l.).

- Direktiva evropskega parlamenta in Sveta št. 2005/60/EC (2005).

Direktivo št. 2001/97/ES je v letu 2005 nasledila tretja direktiva 2005/60/EC. Cilj te direktive je bil predvsem v poenotenju predpisov držav članic EU, ki se nanašajo na področje pranja denarja in financiranje terorizma. Poleg zavezancev iz prejšnjih direktiv (notarji in odvetniki, revizorji, računovodje, davčni svetovalci itn.), vključuje tudi družbe za upravljanje. Podrobno so povzeti ukrepi, ki naj jih zavezanci izvajajo pri skrbnem pregledu stranke (dobro poznavanje svoje stranke, identifikacija stranke, dejanskega lastnika in transakcij, pridobivanje podatkov o namenu in predvideni naravi poslovnega odnosa). Zelo pomembno z vidika trenutnih trendov pri preprečevanju pranja denarja je bilo uvedba novega pristopa, ki temelji na oceni tveganosti (angl. *Risk Based Approach*). Direktiva opredeljuje tudi obravnavo politično izpostavljenih oseb, ki prihajajo iz druge države EU ali iz tretjih držav. V teh primerih morajo države EU izvesti ustrezne ukrepe za upravljanje tveganj in izvesti skrben pregled takšnih strank (Šeme Hočevar, 2007, str. 56−57).

- Direktiva evropskega parlamenta in Sveta št. 2015/849 (2015).

Zadnja objavljena je bila četrta direktiva, in sicer v letu 2015, v veljavo pa bo predvidoma vstopila julija 2017, saj jo morajo do takrat vse države vpeljati v svoje zakone. Četrta direktiva upošteva zadnja priporočila organizacije FATF, izdane v letu 2012. Ključne zahteve, ki jih prinaša ta uredba, so vzpostavitev presoje tveganj za posamezne stranke (angl. *Risk based approach*), izvajanje stalne spremljave strank in njihovega poslovanja,

podrobna opredelitev izvajanja skrbnega pregleda strank in dodatne zahteve glede politično izpostavljenih oseb (The fourth EU Anti Money laundering Directive, 2016).

2.4 FATF (Projektna skupina za finančno ukrepanje)

FATF je bila ustanovljena leta 1989 na vrhu držav G7[3]. Glavni namen FATF je razvoj in stalen napredek zakonodaje, tako mednarodne kot nacionalne, na področju preprečevanja pranja denarja. V letu 1990 so izdali poročilo, ki je vsebovalo 40 priporočil, ki so predstavljale plan za boj proti pranju denarja. Leta 2001 se je področje delovanja organizacije FATF razširilo tudi na preprečevanje financiranja terorizma. Nenehno spreminjanje načinov pranja denarja in financiranje terorizma je zahtevalo prenovo 40 osnovnih priporočil. Zato leto kasneje FATF objavil še 9 posebnih priporočil, s katerimi je na mednarodni ravni okrepil boj proti pranju denarja (Financial Action Task Force, 2016).

Glavne naloge FATF so nadziranje napredka posameznih članic pri implementaciji priporočil in predpisov v nacionalno zakonodajo, spremljanje tehnik in metod pranja denarja ter načinov financiranja terorizma, spodbujanje mednarodnega sodelovanja ter zavzemanje za poenotenje standardov, predpisov in pravil, ki bi omogočali učinkovitejši in uspešnejši boj proti pranju denarja (Šeme Hočevar, 2007, str. 79).

3 UREDITEV PREPREČEVANJA PRANJA DENARJA IN FINANCIRANJA TERORIZMA V SLOVENIJI

Problematika finančnega kriminala v povezavi s pranjem denarja ostaja še naprej aktualna, tveganje pa v zadnjih letih še dodatno povečujejo različne oblike financiranja terorizma. Učinkovit spopad s to problematiko presega okvire nacionalnega delovanja in vse bolj postaja širši, globalni izziv (Svet banke Slovenije, 2008, str. 3).

Na nacionalni ravni je to področje urejeno z Zakonom o preprečevanju pranja denarja in financiranja terorizma in Kazenskim zakonikom, ki sta predstavljena v nadaljevanju. Kaznivo dejanje pranja denarja je bilo v naši nacionalni zakonodaji uzakonjeno v Kazenskem zakoniku leta 1995. Istega leta je začel veljati tudi prvi zakon o preprečevanju pranja denarja in bil Ustanovljen Urad RS za preprečevanja pranja denarja.

3.1 Zakon o preprečevanju pranja denarja in financiranja terorizma

V Sloveniji je bil prvi zakon, ki se je ukvarjal s področjem preprečevanja pranja denarja Zakon o preprečevanju pranja denarja (Ur.l. RS, št. 36/94, št. 63/95, št. 12/96 – ORZPPD28, št. 29/99, št. 79/01, v nadaljevanju ZPPDen), ki je začel veljati 7. julija 1994 in predstavlja temeljni predpis na področju preprečevanja pranja denarja v Sloveniji.

[3] G7 sestavljajo ZDA, Kanada, Japonska, Nemčija, Italija, Francija in Združeno Kraljestvo.

Omenjeni zakon je bil večkrat spremenjen in dopolnjen z do tedaj izoblikovanimi mednarodnimi standardi iz ratificiranih mednarodnih pogodb ter drugimi mednarodnimi predpisi, saj je Slovenija želela zagotoviti postopno združljivost zakonodaje na področju odkrivanja in preprečevanja pranja denarja s pravom EU (Žerjal, 2009, str. 25).

Državni zbor je 21. junija 2007 sprejel nov Zakon o preprečevanju pranja denarja in financiranja terorizma (Ur.l. RS, št. 60/07, 19/10, 77/11, 108/12 – ZIS-E in 19/14, v nadaljevanju ZPPDFT), ki je vključeval zahteve naslednjih direktiv; Direktiva Evropskega parlamenta in Sveta 2005/60/ES, Direktiva Komisije 2006/70/ES in Direktiva 2007/64/ES Evropskega parlamenta in Sveta. Ena glavnih novosti tega zakona je bila uveljavitev pristopa, ki temelji na oceni tveganosti (angl. *Risk based approach*). Skladno s tem imajo zavezanci naloženo obveznost, da izdelajo analizo tveganosti, s katero se oceni tveganost za posamezne skupine strank, poslovnih razmerij, produktov in storitev z vidika možne zlorabe za pranje denarja in financiranja terorizma. Na podlagi pripravljene analize in rezultatov je potem treba izvajati tudi ustrezne ukrepe (Smernice za izvajanje zakona o preprečevanju pranja denarja in financiranja terorizma, b.l.).

Bistvene spremembe, ki jih je ZPPDFT uvedel v slovenski pravni red, so naslednje (Poročevalec državnega zbora, 2007, str. 4−6):

1. Razširjen je krog zavezancev za izvajanje nalog s področja boja proti pranju denarja in financiranju terorizma (primer: organizacije za posredovanje denarja in storitev v plačilnem prometu, družbe za izdajo elektronskega denarja …).
2. Razširitev obveznosti sporočanja sumljivih transakcij, kadar gre za sum financiranja terorizma.
3. Uvedba možnosti ustavitve sumljive transakcije, ko obstajajo razlogi za sum za financiranje terorizma.
4. Uvedba možnosti obravnave strank na podlagi ocene tveganja (priprava ocen in analiz tveganja).
5. Prepoved uporabe anonimnih produktov (računov, hranilnih knjižic na geslo).
6. Prepoved poslovanja z navideznimi bankami.
7. Omejitve poslovanja z gotovino v primerih plačila blaga pri trgovcih v zneskih nad 15.000 EUR.
8. Možnost prepuščanja izvajanja določenih postopkov pregleda stranke tretjim osebam.
9. Podrobnejša je tudi opredelitev mednarodnega sodelovanja z drugimi državami in njihovimi organi, pristojnimi za področje PPDFT.

Po sprejetju prvega ZPPDFT je bil marca 2010 sprejet Zakon o spremembah in dopolnitvah zakona o preprečevanju pranja denarja in financiranja terorizma (Ur.l. RS št. 19/10, v nadaljevanju ZPPDFT-A), ki je začel veljati 27. 3. 2010. Septembra 2011 je bil dopolnjen z Zakonom o dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (Ur.l. RS št. 77/11, v nadaljevanju ZPPDFT-B), nazadnje pa je bil zakon

dopolnjen 17. 3. 2014, ko je bil sprejet Zakon o dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (Ur.l. RS št. 19/14, v nadaljevanju ZPPDFT-C).

Več o sami vsebini zakona je predstavljeno v poglavju 4.1. Zahteve iz Zakona o preprečevanju pranja denarja in financiranja terorizma.

V letu 2016 se pričakuje objava novega, dopolnjenega Zakona o preprečevanju pranja denarja in financiranja terorizma. Podlaga za sprejetje so:

1. Četrta AML direktiva Evropskega parlamenta in Sveta 2015/849 z dne 20. 5. 2015 o preprečevanju uporabe finančnega sistema za pranje denarja in financiranje terorizma (prenos določb v slovenski pravni red).
2. Revidirana Priporočila projektne skupine za finančno ukrepanje (ang. *Financial Action Task Force - FATF*), ki bodo uskladila slovenski pravni red z mednarodnimi standardi.
3. Dosedanje izkušnje pri izvajanju veljavne zakonodaje in ugotovljene potrebe po spremembah (uvedba določenih novosti za učinkovitejši sistem PPDFT).
4. Ugotovitve ocenjevalcev Odbora strokovnjakov Sveta Evrope MONEYVAL ter na podlagi teh s strani Vlade RS sprejet Akcijski načrt za izvršitev priporočil odbora (izvajanje ukrepov za izboljšanje sistema PPDFT).

Ključne večje spremembe v novem zakonu bodo:

- **13. člen:** obveznost dokumentiranja ocene tveganja in posodabljanja na 2 leti;
- **14. člen:** možnost izvedbe poenostavljenega pregleda (predpogoj je, da je ocena tveganja: neznatno);
- **17. člen:** obveznost pregleda pri vsaki transakciji nad 1000 EUR (vsaj delno izvedenimi z elektronskimi sredstvi);
- **22−25. člen:** uvedba možnosti uporabe kvalificiranega digitalnega potrdila tudi za zakonite zastopnike ter preverjanje istovetnosti stranke z uporabo video elektronske identifikacije;
- **31. člen:** vsi poslovni subjekti morajo sami ugotoviti podatke o svojih dejanskih lastnikih (nadzor in sankcije);
- **44. in 46. člen:** določitev načina pregleda stranke (poenostavljen / poglobljen);
- **48. člen:** politično izpostavljene osebe niso zgolj več tuje osebe, temveč tudi domače.

Ostale pomembnejše spremembe še vključujejo: nižanje meje za sporočanje gotovinskih transakcij s 30.000 na 15.000 EUR; pridobitev pooblastil Urada za preprečevanje pranja denarja in financiranja terorizma za izvajanje inšpekcijskega nadzora in uvedba sistema obveščanja o kršitvah (Muzenič, 2015).

Osnutek novega zakona je pripravljen v skladu z najnovejšimi standardi, ki trenutno veljajo na tem področju in ki bo v prihodnje zagotavljal skladnost naše države s strogimi zahtevami, ki veljajo na tem področju.

3.2 Kazenski zakonik

Za vzpostavitev pravne podlage, ki omogoča kazensko preganjanje za primere pranja denarja, je v Kazenskem zakoniku uporabljen 245. člen (Ur.l. RS, št. 91/11-KZ-1B, 50/2012-KZ-1-UPB2), ki obravnava pranje denarja kot kaznivo dejanje zoper gospodarstvo. V tem členu je opredeljeno naslednje:

(1) Kdor denar ali premoženje, za katero ve, da je bilo pridobljeno s kaznivim dejanjem, sprejme, zamenja, hrani, z njim razpolaga, ga uporabi pri gospodarski dejavnosti ali na drug način, določen z zakonom o preprečevanju pranja denarja, s pranjem zakrije ali poskusi zakriti njegov izvor, se kaznuje z zaporom do petih let.
(2) Enako se kaznuje, kdor stori dejanje iz prejšnjega odstavka, pa je hkrati storilec ali udeleženec pri kaznivem dejanju, s katerim je bil pridobljen denar ali premoženje iz prejšnjega odstavka.
(3) Če je denar ali premoženje iz prvega ali drugega odstavka tega člena velike vrednosti, se storilec kaznuje z zaporom do osmih let in denarno kaznijo.
(4) Če je dejanje iz prejšnjih odstavkov storjeno v hudodelski združbi za izvedbo takih dejanj, se storilec kaznuje z zaporom od enega do desetih let in denarno kaznijo.
(5) Kdor bi moral in mogel vedeti, da je bil denar ali premoženje pridobljeno s kaznivim dejanjem, pa stori dejanje iz prvega ali tretjega odstavka tega člena, se kaznuje z zaporom do dveh let.
(6) Denar in premoženje iz prejšnjih odstavkov se vzameta.
Kaznivo dejanje pranja denarja je bilo v naši nacionalni zakonodaji uzakonjeno v Kazenskem zakoniku leta 1995.

4 IZBIRA PROGRAMSKE REŠITVE

Pri izbiri programske rešitve za preprečevanje pranja denarja in financirana terorizma je ključno, da banka zelo dobro preuči čim več rešitev, ki so na trgu in se odloči za tisto, ki je najustreznejša za njeno okolje.

Odločanje o izbiri rešitve je proces, tako Heracleous (1994), ki je organiziran, sistematičen in racionalen ter poteka v naslednjih fazah:

- definiranje problema,
- zbiranje podatkov,
- opredelitev kriterijev,

- iskanje najustreznejše rešitve,
- ocenjevanje in izbira ustrezne rešitve,
- implementacija rešitve in nadzor nad njenim delovanjem.

Pri izbiri rešitve za PPDFT je pomembno vedeti naslednje: osnovni namen programske rešitve za preprečevanje pranja denarja in financiranje terorizma je analiziranje podatkov strank in odkrivanje sumljivih transakcij. Trenutno banke po vsem svetu delajo v smeri večje stabilnosti v globalnih bančnih sistemih. Ta stabilnost je v današnjem času še posebno ogrožena predvsem zaradi hitrega razvoja informacijske tehnologije, povečevanja vpliva globalizacije in zaradi vplivov kriminala in terorizma. Nacionalne skupnosti so se na te grožnje odzvale z različnimi ukrepi (Basel II, The Patriot Act, MIFID, 3 EU regulative on Money laundering …). V finančnih institucijah se porabi veliko časa in energije za implementacijo različnih zakonodajnih okvirjev ter načinov za ugotavljanje in zmanjševanje tveganj za pojav pranja denarja ter financiranja terorizma (FICO Tonbeller, 2016).

Ključno je tudi, da se banka zaveda, da je ustrezna izbira rešitve samo del kompleksnega sistema za preprečevanje pranja denarja, ki ga morajo banke vzpostaviti, v kolikor želijo biti skladne za zakonodajnimi zahtevami. Vsaj tako pomembni kot sama tehnična rešitev so še (KPGM, 2016):

1. Politika upravljanja (urejeni pravilniki z jasno opredeljenimi odgovornostmi in navodili).
2. Zaposleni (izobraženi zaposleni, ki poznajo področje in so kompetentni za odločanje).
3. Procesi (urejeni procesi, ki omogočajo ustrezno izvajanje nalog).
4. Organizacija (ustrezna organizacija enote za preprečevanje pranja denarja (neodvisnost, odgovornost upravi banke).
5. Operativno delo (tukaj lahko nastane potencialna težava preobremenjenosti zaposlenih v primeru prevelikega števila neustreznih zadetkov *(*angl. *false positive hits*).
6. Tveganje in kontrole (ustrezna spremljava tveganj za celotno področje preprečevanja pranja denarja in financiranja terorizma in nadzor nad izvajanjem postopkov).
7. Tehnologija (zaradi naraščajoče kompleksnosti področja PPDFT je zelo pomemben faktor pri zagotavljanju nivoja kakovosti spremljave tudi ustrezna tehnična rešitev).

Ključno pri tem je, da samo nakup rešitve za PPDFT za banke še ne predstavlja skladnosti, ampak je treba pokriti cel spekter delovanja – od procesov, zaposlenih do tehnologije.
Podjetja v finančnem sektorju so zelo odvisna od informacijske tehnologije, ki mora prinašati inovacije, nižati stroške in varovati investicije vlagateljev pred različnimi tveganji. Na podlagi teh zahtev je precejšen del sredstev, ki so namenjeni informacijski tehnologiji (v nadaljevanju IT), usmerjen k zniževanju tveganja pranja denarja in financiranja terorizma (FICO Tonbeller, 2016).

4.1 Zahteve iz Zakona o preprečevanju pranja denarja in financiranja terorizma

Od rešitve za preprečevanje pranja denarja in financiranje terorizma se v prvi vrsti pričakuje, da bo banki omogočala, da doseže skladnost z zakonodajo na tem področju. V tem poglavju bom izpostavil člene iz novega osnutka zakona za PPDFT, katerih skladnost se zagotavlja v okviru rešitve za to področje. Skladnost za ostale člene je potrebno zagotoviti bodisi s kadrovskimi, procesnimi ali organizacijskimi ukrepi.

Finančne institucije od informacijskih rešitev za preprečevanje pranja denarja pričakujejo naslednje (ORACLE, 2010):

- optimalno zaščito pred praksami pranja denarja in financiranja terorizma,
- dinamično vzpostavljanje in spreminjanje »Know your customer« profilov glede na tveganja,
- identificiranje nepričakovanih in nenavadnih aktivnosti,
- avtomatično ugotavljanje obstoječih tveganj.

V spodnji tabeli so predstavljeni poglavitni členi iz Predloga osnutka zakona o PPDFT, ki predstavljajo zahteve za tehnično podporo v rešitvah za preprečevanje pranja denarja (Predlog osnutka ZPPDFT, 2015):

Ob implementaciji rešitev za PPDFT se velikokrat srečujemo z dilemo, katere zahteve pokrivamo s to rešitvijo in kje v zakonu se te zahteve nahajajo. Tabela 1 prikazuje, v katerih členih se nahajajo ključne zahteve, ki so jih banke dolžne izvajati in za zagotovitev skladnosti katerih se uporabljajo rešitve za preprečevanje pranja denarja.

Tabela 1: Zahteve v osnutku novega ZPPDFT

Št. čl.	Opis člena	Zahteva
12	Naloge in obveznosti zavezancev	1. Izdelava ocene tveganja; 2. vzpostavitev politik, kontrol/nadzornih mehanizmov; 3. izvajanje ukrepov za poznavanje stranke; 4. sporočanje predpisanih in zahtevanih podatkov; 5. imenovanje pooblaščenca; 6. skrb za redno strokovno usposabljanje; 7. priprava seznama indikatorjev za prepoznavanje strank in transakcij;

se nadaljuje

Tabela 1: Zahteve v osnutku novega ZPPDFT (nad.)

Št. čl.	Opis člena	Zahteva
12	Naloge in obveznosti zavezancev	8. zagotovitev varstva in hrambe; 9. izvajanje ukrepov odkrivanja in preprečevanja pranja denarja; 10. izvajanje drugih nalog in obveznosti.
13	Ocena tveganja za pranje denarja in financiranja terorizma	Izdelava ocene tveganja (strank, transakcij, produktov …) in posodobitev le teh vsaki 2 leti oziroma ob spremembi procesa/uvedbi novega produkta.
14	Neznatno in povečano tveganje za pranje denarja in financiranje terorizma	Identifikator za neznatno ali povečano tveganje na stranki, produktu, transakciji itd.
15	Obvladovanje tveganj pranja denarja in financiranja terorizma	Vzpostavitev kontrol in postopkov za obvladovanje tveganj (scenariji, parametri …).
16	Sestavni deli pregleda stranke	Uporaba podatkov o namenu in predvideni naravi poslovnega razmerja in redno spremljanje poslovnih aktivnosti, ki jih izvaja stranka (upoštevajoč: višino sredstev, vrednost premoženja ali obseg transakcij, čas trajanja poslovnega razmerja in skladnost poslovanja z namenom sklenitve poslovnega razmerja. Izpis analiz, listin ali podatkov, ki dokazujejo ustreznost izvedenih kontrol pregleda stranke.
17	Obveznost pregleda stranke	Obveznost pregleda stranke se pojavi ob sklepanju poslovnega razmerja, pri transakciji nad 15.000 EUR, vedno, kadar obstaja sum na pranje denarja.
18	Pregled stranke pri sklenitvi poslovnega razmerja	Uporaba podatkov o namenu in predvideni naravi poslovnega razmerja in redno spremljanje poslovnih aktivnosti, ki jih izvaja stranka.
19	Pregled stranke pri izvajanju transakcij	Preverjanje stranke pred izvršitvijo transakcije.
20	Neizpolnitev obveznosti pregleda stranke	Prepoved sklenitve poslovnega razmerja oziroma prekinitev poslovnega razmerja in obveščanje urada o sumljivi transakciji.
21	Delna opustitev pregleda stranke v zvezi z elektronskim denarjem	Delna opustitev pregleda v primerih, ko največji znesek mesečnih transakcij ne presega 500 EUR, obvezna spremljava transakcij.

se nadaljuje

Tabela 1: Zahteve v osnutku novega ZPPDFT (nad.)

Št. čl.	Opis člena	Zahteva
22	Ugotavljanje in preverjanje istovetnosti stranke	Dostop do zunanjih baz podatkov (registri …).
23	Ugotavljanje in preverjanje istovetnosti pooblaščenca fizične osebe	Podatki o osebnem dokumentu.
24	Ugotavljanje in preverjanje istovetnosti pooblaščenca pravne osebe	Podatki o osebnem dokumentu, izjava.
25	Ugotavljanje in preverjanje istovetnosti na podlagi kvalificiranega digitalnega potrdila	Podatek o uporabi kvalificiranega digitalnega potrdila.
26	Ugotavljanje in preverjanje istovetnosti pravne osebe	Povezava do poslovnega, sodnega ali drugega javnega registra.
29	Dejanski lastnik gospodarskega subjekta	Informacija o lastnikih (vneseni podatki oziroma podatkih iz zunanjih baz).
30	Dejanski lastnik drugih poslovnih subjektov, ustanov, pravnih subjektov tujega prava	Informacija o lastnikih (vneseni podatki oziroma podatkih iz zunanjih baz).
31	Obveznosti poslovnih subjektov	Dostopnost podatkov v poslovnem registru.
32	Vpis podatkov o dejanskih lastnikih v poslovni register Slovenije	Dostopnost podatkov o dejanskih lastnikih v poslovnem registru.
35	Nabor podatkov	Opredelitev nabora podatkov, ki jih je potrebno zbirati/preverjati.
36	Skrbno spremljanje poslovnih aktivnosti	Spremljanje in preverjanje skladnosti strankinega poslovanja z njenim običajnim obsegom poslovanj, preverjanje in posodabljanje pridobljenih listin in podatkov o stranki.
37	Obravnava neobičajnih transakcij	Beleženje in hranjene ugotovitev o sumljivih transakcijah. Upoštevanje in posebna obravnava transakcij v določenih primerih (visoko tvegane tretje države …).
45	Izvajanje poenostavljenega pregleda stranke	Upoštevanje nabora podatkov, potrebnih za izvedbo poenostavljenega pregleda stranke.

se nadaljuje

Tabela 1: Zahteve v osnutku novega ZPPDFT (nad.)

Št. čl.	Opis člena	Zahteva
46	Izvajanje poglobljenega pregleda stranke	Upoštevanje nabora podatkov, potrebnih za izvedbo poglobljenega pregleda stranke.
47	Kontokorentna bančna razmerja s kreditnimi institucijami tretjih držav)	Dodatno pridobivanje podatkov (primer: datum izdaje dovoljenja za opravljanje bančnih storitev).
48	Politično izpostavljene osebe	Obvezna vzpostavitev preverjanja ali je stranka politično izpostavljena oseba.
50	Pregled strank iz visoko tveganih tretjih držav	Zahteva za pridobitev dodatnih podatkov o dejavnosti, namenu in predvideni poslovni dejavnosti stranke.
51	Prepoved uporabe anonimnih produktov	Prepoved odpiranja in vodenja anonimnih računov ali hranilnih knjižic na geslo, ki posredno ali neposredno prikrivajo identiteto stranke.
53	Prepoved poslovanja z navideznimi bankami	Preverjanje v »sanction« listah.
54	Omejitev gotovinskega poslovanja	Prepoved prejetja plačila v gotovini nad 5000 EUR za prodajo blaga/storitev (tudi povezanih transakcij).
55	Obveznost sporočanja gotovinskih transakcij	Obveznost poročanja transakcij na podlagi členov iz tega zakona (primer: transakcije nad 15.000 EUR).
56	Obveznost sporočanja sumljivih transakcij in roki	Kontrola poročanja in doslednost glede rokov oddaje poročil.
57	Zadrževanje izvršitve sumljive transakcije	Beleženje informacij in časa obdelave sumljive transakcije (zadrževanje se lahko izvaja največ 24 ur).
74	Obveznost sestave in uporabe seznama indikatorjev	Priprava indikatorjev (scenarijev) za prepoznavanje strank, za katere obstaja sum pranja denarja.
108	Prepoved razkritja	Zaščitenost rešitev za preprečevanje pranja denarja.
115	Rok hrambe podatkov pri zavezancu	Hramba podatkov za določen rok (primer: 5 let po preteku poslovnega razmerja).
116	Podaljšanje roka hrambe podatkov	Urad, policija, tožilstvo lahko zahteva podaljšanje roka hrambe za dodatnih 5 let.
147	Interni sistem obveščanja o kršitvah	Vzpostavitev sistema za obveščanje o kršitvah.

Pri tem je treba poudariti, da se ob grožnjah v današnjem času vse bolj uveljavlja »holistični« pristop k identifikaciji potencialnih tveganj, ki obsega uporabo različnih rešitev in povezanost različnih sistemov za preprečitev dejanj pranja denarja in financiranja terorizma. Silosne rešitve niso več primerne za preprečitev dovršenih napadov, ki se lahko odvijajo v več poslovnih divizijah na različnih kanalih, ki jih stranke uporabljajo. Dodatno se je za te rešitve izkazalo, da povzročajo precej velike stroške, saj zakonodajne spremembe zahtevajo nadgradnje v različnih sistemih, ki med seboj niso povezani (FICO Tonbeller, 2016).

V nadaljevanju bom predstavil rešitve in načine, s katerimi so te zahteve rešili pri podjetju FICO Tonbeller.

4.2 Opis rešitev za PPDFT

V tem poglavju so predstavljene in razložene osnovne funkcionalnosti rešitev za preprečevanje pranja denarja in financiranja terorizma. Razumevanje teh funkcionalnosti pripomore k lažji komunikaciji s ponudniki rešitev za PPDFT v procesu odločevanja oziroma izbire rešitve. Za proces odločanja je ključno, da se banka s ponudnikom čim bolj podrobno pogovori o pričakovanjih rešitve in morebitnih dilemah kako integrirati ponudnikove rešitve v bančno okolje.

4.2.1 Opis rešitve in splošne značilnosti

Za referenčno predstavitev rešitve bomo prikazali rešitev podjetja FICO Tonbeller. Rešitev ponuja širok spekter rešitev za vzpostavitev učinkovitega nadzora nad preprečevanjem pranja denarja in financiranja terorizma. Koncept, kjer se lahko za rešitev določene zahteve uporablja popolnoma neodvisno rešitev, je zastarel in ga je treba zamenjati, saj so trenutni izzivi, ki se pojavljajo na področju preprečevanja pranja denarja in financiranja terorizma, tako medsebojno povezani in odvisni, da je potreben celovit pristop k iskanju rešitve teh izzivov (FICO Tonbeller, 2016).

Trenutne zahteve na področju preprečevanja pranja denarja in financiranja terorizma lahko, po FICO Tonbeller (2016), strnemo v naslednje sklope:

1. Skladnost z zakonodajnimi zahtevami in internimi pravili.
2. Prepoznavanje, beleženje in obdelava vseh ugotovljenih kršitev.
3. Doseganja transparentnosti poslovanja v mednarodnem okolju.
4. Prepoznavanje in vzpostavitev ocene tveganj.
5. Planiranje, vzpostavitev in nadzor ukrepov za preprečevanje pranja denarja.
6. Omogočanje strateških odločitev za omejitev tveganja pranja denarja.
7. Priprava poročil za vodstva podjetij/bank.

Za pokrivanje teh področij so pri FICO Tonbellerju pripravili nabor spodaj opisanih programskih rešitev, ki omogočajo bankam zagotavljati kvaliteten nivo nadzora nad tveganji pred PPDFT.

Na podlagi pregleda v nadaljevanju navedenih rešitev, ki jih podjetje FICO Tonbeller ponuja za soočanje s tveganji na področju poslovanja finančnih institucij, vidimo, da gre za zelo kompleksno področje. Vedno bolj postaja tudi jasno, da je za učinkovito spoprijemanje s temi tveganji in zmožnost zagotavljanja skladnosti z zakonodajo na tem področju, potrebno poseči po visoko specializiranih tehničnih rešitvah. Za celovito zaščito v finančni instituciji je priporočljivo posedovati in uporabljati nabor spodaj naštetih rešitev.

4.2.2 Opis funkcionalnosti rešitve za poznavanje strank

Ko banka pridobi novo stranko mora iz naslova poznavanja stranke pridobiti precej informacij o njej. Čeprav je s strani strank to večkrat videno kot odvečno delo ali celo poseg v zasebnost, je cilj tega vedno to, da se stranko čim bolj zavaruje. Na primer, če stranka pove, da nikoli ne izvaja transakcij večjih od 5000 EUR, se lahko ta nastavitev vnese v bančne sisteme in se v primeru zlorabe takšno transakcijo avtomatično ustavi. Varnost in poznavanje strank postajata prioriteta saj je število zlorab, kot je na primer kraja identitete ali pa zloraba bančnih kartic, v porastu (Jones, 2013).

Iz zgoraj omenjenih vzrokov je ustrezno identificiranje in poznavanje stranke izredno pomemben korak pri preprečevanju pranja denarja in financiranja terorizma. Ko banka dobi novo stranko in ji omogoči delo z njenimi produkti, ji s tem omogoči tudi dostop do domačega in mednarodnega okolja. Zaradi tega je ključno, da banke poznajo in razumejo stranko, predvsem namen njenega poslovanja, finančno situacijo, vire financiranja in tveganja, ki jih ta stranka za banko predstavlja.

Za zagotavljanje zgoraj zapisanega Siron KYC rešitev (angl. *Know Your Customer* – KYC, poznavanje svoje stranke) omogoča bankam uporabo dinamičnega vprašalnika za stranke, vgrajenega preverjanja politično izpostavljenih oseb (angl. *Politically Exposed Person - PEP*), preverjanja iz list sumljivih oseb, preverjanja upravičenih lastnikov (angl. *beneficial owner*) in avtomatično beleženje revizijske sledi za vse naštete procese. Poleg tega rešitev omogoča tudi povezovanje preko spletnih servisov neposredno z bančnimi sistemi (FICO Tonbeller, 2016).

Rešitve za poznavanje strank morajo nuditi celoten pregled nad stranko in hkrati podpirati proces, s katerim banke zagotavljajo, da imajo o stranki vse potrebne informacije. Trenutek, ko je sprejeta odločitev ali bo banka novo stranko sprejela ali zavrnila, je zelo pomemben, saj se lahko s temeljitim pregledom stranke izogne tveganju pranja denarja. Na tej točki je ključno, da banke pridobijo informacije o strankinem preteklem poslovanju,

izvoru sredstev, ki jih stranka ima, produktih, ki jih stranka uporablja ali ponuja, saj si na ta način lahko ustvari ustrezen profil stranke. Predvsem je treba biti pozoren na to, da rešitve ponujajo ustrezne kontrole za primere podjetij, ustanovljenih v davčnih oazah, pri politično izpostavljenih osebah in pri strankah, ki so rezidenti držav s pomanjkljivimi kontrolami na področju preprečevanja pranja denarja in financiranja terorizma. Prav tako morajo rešitve omogočiti preverjanje, ali stranka iz sumljivih držav prejema sredstva ali se ukvarja s tako vrsto posla, za katero je znano, da je velika verjetnost, da bi se lahko pojavilo povišano tveganje za pranje denarja (FICO Tonbeller, 2016).

Pri izbiri in uvajanju rešitve za poznavanje stranke je priporočljivo biti pozoren na naslednje:

- Kompatibilnost rešitve z vidika povezovanja z obstoječimi bančnimi sistemi, ki so v veliko primerov starejšega izvora in imajo omejene možnosti povezovanja preko sodobnih rešitev kot so spletni vmesniki.
- Čas trajanja obdelave za celoten portfelj strank mora biti izveden v največ 30 minutah (ne glede na to, da se običajno izvaja izven delovnega časa banke).
- Hitrost obdelave posameznega zahtevka preko spletnega vmesnika, ki se običajno izvede preko rešitev, ki se uporabljajo v poslovnih enotah, mora biti zaključena v najkrajšem možnem času (največ 2 sekundi).
- Priporočljivo je, da se vsa potrebna preverjanja za poznavanje stranke izvedejo znotraj te rešitve in da ni potrebe po dodatnem ročnem preverjanju v ostalih bazah podatkov (primer: poseben register za stranke, ki so blokirane na drugih bankah).
- Ključno pri uvajanju rešitve pa je tudi ustrezno terminološko poimenovanje polj in poenotenje v vseh sistemih (na primer sistem, ki se uporablja v poslovni enoti; bančni sistem, ki hrani vse podatke o strankah; rešitev za poznavanje strank idr.).
- Zaradi krepitve zakonodaje na področju varovanja osebnih podatkov mora rešitev za poznavanje strank imeti urejeno tudi ustrezno beleženje vseh sprememb in vpogledov v osebne podatke strank.

Rešitev za poznavanje stranke je ključna kontrolna točka pred vstopom strank v bančno okolje in je zato izredno pomembna pri preprečevanju pranja denarja in financiranju terorizma. Tudi zaradi tega, je potrebno posebno pozornost ob izbiri in implementaciji, nameniti tej rešitvi.

4.2.3 Opis funkcionalnosti rešitve za preprečevanje pranja denarja

Pranje denarja omogoča zločincem spremeniti nezakonito pridobljena sredstva v zakonita sredstva. Tega si želijo zato, da lahko ta denar potem porabljajo brez strahu, da bi jih lahko povezali s kriminalnimi dejanji, pri katerih so do teh sredstev prišli. Poleg tega pa oblastem uspešno pranje denarja onemogoči postopke, s katerimi bi zločincem ta denar lahko odvzeli. Kot smo že omenili, pranje denarja poteka v treh korakih: plasma, ustvarjanje plasti in integracija. Pri tem je plasma najtežji korak, saj zajema prenos sredstev v bančni

sistem. Pri ustvarjanju plasti gre za prenose med različnimi računi, medtem ko gre pri integraciji že za porabo teh sredstev, pri čemer je težko ali celo nemogoče določiti izvor teh sredstev.

Za preprečevanje pranja denarja rešitev Siron AML omogoča bankam spremljavo transakcij na podlagi različnih scenarijev, ki omogočajo identifikacijo sumljivih transakcij, ki jih lahko strokovnjaki v bankah sami določajo in spreminjajo. Poleg tega se s pomočjo rešitve izvede tudi profiliranje stranke, sistem pa potem samodejno obvešča o odstopanjih od običajnega obnašanja stranke. Za lažje delo bančnih uslužbencev rešitev omogoča slikovno predstavitev povezav med transakcijami, strankami, računi in lokacijami, ki so v veliko pomoč pri odkrivanju shem pranja denarja (FICO Tonbeller, 2016).

Siron AML je neodvisna uporabniška rešitev za analiziranje in spremljanje neobičajnih finančnih transakcij. Ta rešitev uporabnikom omogoča naslednje (FICO Tonbeller, 2016):

1. Skladnost z mednarodnimi standardi za preprečevanje pranja denarja in financiranje terorizma (3. in 4. EU direktiva s področja preprečevanja pranja denarja in financiranja terorizma, FATF 40+9 priporočil, Ameriški domovinski zakon (angl. *USA Patriot act*)).
2. Spremljava in identifikacija sumljivih transakcij in zagotavljanje metod za minimiziranje operativnih tveganj na podlagi izločanja samo resnično ustreznih zadetkov (učinkovito upravljanje nastavitev, da se izločijo nepravilni zadetki (angl. *false positives*).
3. Analitične rešitve, ki uporabniku enostavno in jasno predstavijo tveganja za preprečevanje pranja denarja in financiranja terorizma za vsako posamično stranko.
4. Omogočena je integracija procesov in opozoril za čim učinkovitejšo obravnavo zaznanih sumljivih transakcij.
5. Samodejna priprava poročil v zahtevnih strukturah in formatih.
6. Zaradi intuitivnega vmesnika lahko pooblaščenci za pranje denarja sami pripravljajo in spreminjajo scenarije.
7. Rešitev že omogoča uporabo določenih pred-nastavljenih scenarijev.
8. Vizualizacija povezav med transakcijami, strankami, računi in različnimi geografskimi področji je na voljo za lažjo zaznavo shem pranja denarja.
9. Siron AML je povezljiv z vsemi večjimi osnovnimi bančnimi rešitvami.

Ob različnih statistično-analitičnih procesih, ki jih rešitev podpira, lahko pooblaščenci za pranje denarja nastavljajo lastne kriterije in tipologije, ki jim lahko pomagajo prepoznati različne sheme pri pranju denarja, medtem ko se podatki o stranki primerjajo s kriteriji in tipologijami. V primeru ujemanja se transakcijo/stranko označi kot sumljivo in jo je treba podrobneje preveriti. Za lažje delo pooblaščencev pranja denarja se zadetki z opisi vseh sumljivih indikatorjev prikažejo znotraj enega opozorila in s tem omogočijo lažjo obravnavo zaznave sumljivih aktivnosti. Tak način priprave opozoril v veliki meri

pripomore v zmanjšanju nepravilnih zadetkov (angl. *false positives*). Modul Siron AML dinamično izdeluje profile za vsako stranko oziroma skupino strank in zapisuje posamično kot tudi skupinsko obnašanje v določenem časovnem obdobju. Ker je vsako stranko treba spremljati skozi celotno obdobje njenega razmerja s finančno institucijo, je zelo pomembna tudi povezava med AML- modulom, ki zagotavlja to spremljavo, in KYC-modulom, ki hrani začetno stanje stranke. Ob nenehnem spremljanju strankinih aktivnosti nas rešitev takoj opozori, če se pojavijo velika odstopanja od podatkov, ki jih je ob odprtju poslovnega odnosa navedla stranka (FICO Tonbeller, 2016).

Pri izbiri in uvajanju rešitve za preprečevanje pranja denarja je priporočljivo biti pozoren na naslednje:

- Da rešitev omogoča uvoze podatkov v različnih oblikah. Odločitev banke je ali bo podatke pripravljala neposredno iz plačilnih sistemov ali pa iz podatkovnih skladišč, kjer so podatki o transakcijah na voljo še za druge namene (poslovne analize,…).
- Veliko pozornost je potrebno usmeriti tudi v planiranje in preučitev količine transakcij, ki jih je rešitev sposobna obdelati. Upoštevati je potrebno pridobitev podjetja z zelo velikim številom transakcij ali pa pridružitev druge banke in prevzem njenih transakcij.
- Čas trajanja preverjanja vseh transakcij, čeprav izven delovnega časa ne sme preseči 30 minut.
- Priporočljivo je, da rešitev ob zadetku omogoča neposreden vpogled in po potrebi spremembo osnovnih podatkov strank, ki se nahajajo v rešitvi za poznavanje stranke, saj se na ta način pohitri obdelava zadetkov in ni potrebe po uporabi dveh rešitev na operativnem nivoju.

4.2.4 Opis funkcionalnosti rešitve za spremljavo sumljivih transakcij

Poleg pranja denarja se v zadnjem času izredno krepijo tudi ukrepi za odkrivanje financiranja terorizma. V preteklosti so to vlogo izvajali nacionalni varnostni uradi in različne agencije ter policija in vojska, sedaj pa so se v to vključile tudi banke, zavarovalnice in določena podjetja. Glede na vedno višjo stopnjo prisotnosti terorizma se pričakuje, da se bo zakonodaja tudi za banke na tem področju še stopnjevala. Kršenje te zakonodaje pa bi pomenilo predvsem velik udarec za ugled katerekoli banke, ki želi sodelovati v mednarodnem finančnem okolju. Omejitve, ki jih zaradi tveganja financiranja terorizma morajo banke upoštevati, izhajajo iz zelo različnih virov: država izvora, poslovni partnerji ali pa sami izdelki, s katerimi se trguje. Za preprečevanje pranja denarja in financiranja terorizma Siron EMBARGO rešitev omogoča takojšnje (real time) preverjanje transakcij s pomočjo mednarodnih sankcijskih list, ki jih pripravljajo Urad za nadzor tujih sredstev (OFAC) ali pa internih list, ki so v domeni bank. Iskanje zadetkov poteka s kompleksnimi iskalnimi mehanizmi, katerih namen je zagotoviti čim bolj točne zadetke.

Vsak zadetek vsebuje povezavo na listo ali scenarij, ki je bil podlaga za ustavitev transakcije, kar omogoča hitrejšo in kvalitetnejšo obdelavo transakcij. Da se banka ne ukvarja s prevelikim številom neupravičeno ustavljenih transakcij, rešitev ponuja možnost vzpostavitve poslovnih pravil (angl. *white listing*), na primer podjetij, katerih ime vsebuje ime kakšne teroristične organizacije, a lahko banka naredi pravilo, da se za to stranko transakcije ne ustavljajo. Zaradi izredno občutljivih informacij in časovnih presekov se v Siron EMBARGO rešitvi vse aktivnosti, ki se izvedejo, hranijo kot revizijska sled (FICO Tonbeller, 2016).

Siron EMBARGO je tako v osnovi neodvisna uporabniška rešitev za preverjanje ali se podatki v transakcijah ujemajo s podatki, iz katere izmed predpisanih sankcijskih list in proženje opozoril ter ustavitev takih transakcij. Uporabnikom omogočajo naslednje (FICO Tonbeller, 2016):

1. Skladnost z zakonodajnimi zahtevami, ki pokrivajo boj proti mednarodnemu terorizmu in zamrznitvi sredstev (primer: EU regulativa 2580/2001 in 881/2002).
2. Takojšnje preverjanje (real-time) pošiljateljevih (prejemnikovih) podatkov s sankcijskimi listami (OFAC lista - Office of foreign assets control, CFSP lista – Common foreign security policy …).
3. Rešitev podpira obdelavo SWIFT sporočil (SWIFT MT in SWIFT MX), SEPA sporočil (ISO 20022) in ostalih formatov plačilnih sporočil (Merva, WBI-FN …).
4. Razviti so kompleksni iskalni mehanizmi (iskanje po točno določenih zapisih, iskanje po delnih zapisih (angl. *fuzzy search*) za identifikacijo transakcij v povezavi s terorističnimi dejavnostmi.
5. Transakcija, ki se ustavi zaradi sumljivih indikatorjev, ima označeno, zaradi katerih besed ali besednih sklopov v transakciji se je ustavila in še neposredno ob tej besedi ima povezavo na vpis v sankcijski listi, ki je podlaga za ustavitev te transakcije – s tem se zelo pohitri sam proces obdelave sumljivih transakcij.
6. Možnost vnosa izjem, za katere se transakcije ne ustavljajo, ker so na beli listi (angl. *white list*), in dodajanje poslovnih pravil, ki zmanjšajo napačne zadetke (angl. *false positives*).
7. Revizijska sled za vse sistemske kontrole, delovne korake in odločitve sprejete v sistemu.

Ena glavnih lastnosti Siron EMBARGO rešitve je integracija mednarodnih sankcijskih list, kot na primer OFAC (Office of foreign assets control), CFSP (Common foreign security policy), HMT (Her majesty treasury), German federal gazette in UN resolution lists. SironEMBARGO prav tako podpira plačljive liste, ki jih je moč kupiti na trgu, kot so World check, Dow Jones Factiva ali World compliance. Rešitev omogoča, da se s pravili določa, katere transakcije se kontrolirajo, s katero listo (primer: transakcije v dolarjih se preverjano z OFAC listo). Ključna funkcionalnost rešitve je, da preverja vse transakcije z

morebitnimi povezavami z mednarodnim terorizmom in jih v primeru odkritja povezav tudi ustavi. Preverjajo se podatki o pošiljatelju in prejemniku v plačilu (ime, vzdevek …). V primeru, da se odkrije povezava med podatki v plačilu in podatki iz sankcijskih list, se takšno plačilo nemudoma ustavi in s tem prepreči kakršnokoli nadaljnje razpolaganje s temi sredstvi. Zelo pomembno pa je tudi, da so vse transakcije, ki niso bile identificirane kot sumljive, čim prej obdelane.

Učinkovito iskanje pravilnih zadetkov (angl. *true positives*) je omogočeno tudi z uporabo naprednih iskalnih rešitev, kot je na primer tako imenovan »fuzzy search« s pomočjo katerega lahko rešitev identificira povezave med plačilom in listo tudi v primeru, da se za imena uporablja okrajšave, zamenjave črk v imenih spremenjeno zaporedje imen idr. Uporaba teh naprednih iskalnih rešitev omogoča uporabnikom rešitve nastavitev minimalnih zahtev, ki jih želijo doseči pri iskanju povezav med podatki v plačilih in sankcijskih listah, te nastavitve pa lahko občutno zmanjšajo število nepravilnih zadetkov (angl. *false positives*). Dodatno lahko k temu pripomorejo tudi uporabe belih list (angl. *white lists*), ki omogočijo osebam, ki se ukvarjajo z zadetki, še bolj točne zadetke, na katere se lahko slednji v celoti koncentrirajo (FICO Tonbeller, 2016).

Pri izbiri in uvajanju rešitve za spremljavo sumljivih transakcij je priporočljivo biti pozoren še na naslednje:

- Hitrost obdelave posamezne transakcije (največ 2 sekundi) in beleženje vseh korakov ob preverjanju transakcije. Slednje je pomembno, ker je čas obdelave pri transakcijah kritična komponenta.
- Pridobitev scenarijev s strani ponudnika rešitve. Pri preprečevanju pranja denarja veliko pravil sloni na preteklih izkušnjah, zato lahko ponudniki, ki imajo na trgu postavljenih več rešitev, nudijo tudi boljšo podporo pri postavitvi scenarijev.
- Priporočljivo je opraviti poglobljeno analizo za vzpostavitev tako imenovanih belih list (angl. *white list*), ki izločijo transakcije, ki bi bile neupravičeno prikazane kot sumljive. Tak primer je podjetje ETA Kamnik, ki se bi na listi znašel zaradi teroristične organizacije ETA. Ta funkcionalnost lahko bistveno pripomore k zmanjšanju delovne obremenitve v različnih oddelkih v banki (na primer: plačilni promet).

Izbira in vzpostavitev rešitve za spremljavo sumljivih transakcij si zasluži posebno pozornost, ker so v primerih kršitve zagrožene precej visoke kazni, poleg tega pa banka tvega tudi izgubo ugleda, kar lahko zelo negativno vpliva na njeno uspešnost poslovanja.

4.2.5 Opis funkcionalnosti rešitve za pripravo ocene tveganj

Rešitev za pripravo ocene tveganj zaključuje nabor rešitev, ki so potrebne za učinkovito obvladovanje področja preprečevanja pranja denarja in financiranja terorizma.

Večina novih regulativ s področja pranja denarja in financiranja terorizma (kot so FATF priporočila, 4. EU direktiva za preprečevanje pranja denarja in druge), zahteva vzpostavitev vedno strožjih ukrepov na področju pranja denarja. Zelo pomemben element pri preprečevanju pranja denarja je tudi priprava ocen tveganj. Slednje je podlaga za vse nadaljnje aktivnosti, ki jih morajo finančne institucije vzpostaviti na tem področju: vzpostavitev varnostnih politik, priprava internih pravil in kontrol, identifikacija zahtev, potrebnih za pripravo pravil (scenarijev), potrebnih za preprečitev pojava tveganj idr. Tipičen primer, ki ga je treba izvesti, je ocena tveganja za vse fizične in pravne osebe, ki pove banki, kolikšno je potencialno tveganje te stranke za primer pranja denarja ali financiranja terorizma. Na podlagi te ocene tveganja morajo nato za vsako kategorijo biti vzpostavljeni določeni ukrepi, s katerimi se omeji samo tveganje in prepreči škoda v obliki raznih glob ali izgube ugleda. Za pripravo ocene tveganj nam Siron RAS rešitev ponuja možnost identifikacije, kategorizacije, ocenitve ter vzpostavite ukrepov za preprečevanje pojavov tveganj.

Funkcionalnosti, ki jih morajo imeti rešitve za to področje, zajemajo (FICO Tonbeller, 2016):

1. Funkcionalnost za identifikacijo, kategorizacijo in oceno tveganj.
2. Prikaz organizacijske strukture, nabora produktov in kategorij strank in za vsako izmed njih opredeljena ocena tveganja.
3. Opis in možnost preverjanja ocene tveganja za vsako organizacijsko enoto, produkt in skupino strank.
4. Možnost izvedbe analiz stopnje ogroženosti za vsako organizacijsko enoto, produkt in skupino strank.
5. Neposredne povezave z rešitvijo za preverjanje poznavanja strank, rešitvijo za preprečevanje pranja denarja in rešitvijo za spremljavo sumljivih transakcij za namen sprotnega spremljanja in posodabljanja scenarijev.
6. Podrobno zapisovanje vseh aktivnosti, ki so bile izvedene v sistemu za zagotovitev ustreznih revizijskih sledi.

Pri izbiri in uvajanju rešitve za pripravo ocene tveganj je priporočljivo biti pozoren še na naslednje:

- Zagotoviti je potrebno povezljivost rešitve za oceno tveganj z drugimi procesnimi orodji v banki, ki bodo morale imeti oceno tveganja vključeno v različne odobritvene postopke.
- Ukrepi, ki jih bo potrebno vzpostaviti za omejitev tveganj pranja denarja in financiranja terorizma v bankah, si bodo zaradi enakega zakonodajnega okvirja precej podobni. Zato se priporoča, da banka skupaj s ponudnikom te ukrepe vpelje v rešitev in tako zagotovi uporabo najboljše prakse.

Na podlagi zadnjih zahtev, ki jih je vzpostavila Evropska unija z izdajo 4. AML direktive bo rešitev za pripravo ocene tveganj postala ena izmed ključnih rešitev v bankah (predpisana je obveznost posodabljanja ocene tveganj na 2 leti).

Na podlagi pregleda zgoraj navedenih rešitev, ki jih podjetje FICO Tonbeller ponuja za soočanje s tveganji na področju poslovanja finančnih institucij, vidimo, da gre za zelo kompleksno področje. Vedno bolj postaja tudi jasno, da je za učinkovito spoprijemanje s temi tveganji in zmožnost zagotavljanja skladnosti z zakonodajo na tem področju treba poseči po visoko specializiranih tehničnih rešitvah.

4.3 Ključni aspekti, ki jih je treba upoštevati pri izbiri rešitve za področje PPDFT

Pri vsaki izbiri novih tehničnih rešitev se ljudje, ki se odločajo o nakupu, srečujejo s podobnimi dilemami: ali rešitev pokriva vse zahteve, ali je rešitev uporabniku prijazna, ali je cena rešitve ustrezna in še številne druge. V primeru izbire rešitve za področje preprečevanja pranja denarja (v nadaljevanju PPD) pa lahko, zaradi potencialnega velikega vpliva na ugled finančne institucije, napaka pri odločitvi prinese zelo hude posledice.

Ključne zahteve, ki bi jih morale pokrivati rešitve za preprečevanje pranja denarja, so naslednje (ORACLE, 2010):

1. Zadostitev zakonodajnim zahtevam

Rešitve za preprečevanje pranja denarja morajo zaznati in onemogočiti potencialne sumljive aktivnosti. Zakonodajalci zelo natančno predpisujejo, kaj je treba spremljati, in postavijo merila, ki veljajo za celotno industrijo.

2. Pokrivanje celotne banke

Pralci denarja v svojih metodah uporabljajo vedno bolj iznajdljive načine pranja denarja, kar pomeni, da dejanj ne izvedejo samo v eni poslovni enoti, ampak poskušajo na več različnih. Prav tako poskušajo prikriti svoje delovanje z uporabo več računov ali uporabo več različnih vrst produktov. Prav zaradi tako širokega področja pranja denarja je treba imeti rešitve, ki pokrivajo celoten spekter tveganj na ravni cele banke.

3. Hitro zaznavanje vseh sumljivih aktivnosti

Sodobne rešitve morajo biti sposobne nenehno spremljati vse stranke, račune in transakcije. Omogočeno mora biti iskanje novih vzorcev in sumljivih aktivnosti vsakodnevno ali v nekaterih primerih tudi znotraj dneva (spremljanje pred izvršitvijo).

4. Uporabniku prijazna rešitev

Rešitev za preprečevanje pranja denarja mora biti prilagodljiva, enostavna za uporabo in enostavna za spreminjanje. Novi produkti, ki so različno tvegani, se na trgu pojavljajo v vedno večjem številu in prav tako se hitro spreminjajo razmere na trgu.

5. Zagotavljati dolgoročno stroškovno učinkovito rešitev

Ker je uvedba PPD-rešitve v banko zahtevna, je treba upoštevati, da bo tudi dolgoročno stroškovno učinkovita, kar pomeni, da se že na začetku predvideva rast števila podatkov in tudi podporo tehničnim in finančnim inovacijam, ki se pričakujejo v prihodnjem obdobju.

6. Uporaba najboljših praks

Sistemi za PPD potrebujejo za svoje delovanje različne metode, s katerimi lahko odkrivajo pralce denarja. Če se uporabijo izkušnje več igralcev na trgu, so te metode veliko bolj izpopolnjene in učinkovite.

Poleg že zgoraj naštetih ključnih dejavnikov, ki jih je treba pri izbiri rešitve za preprečevanje pranja denarja vzeti v obzir, so vsekakor zelo pomembni tudi naslednji: na kakšen način se podatke uvaža v sistem, kakšne revizijske sledi sistem zagotavlja, na kakšen način se izvaja vzdrževanje aplikacije in ali se lahko novo rešitev poveže z ostalimi varnostnimi rešitvami, ki jih banka uporablja (ORACLE, 2010).

Poleg vseh zgoraj naštetih dejavnikov, ki jih je treba upoštevati, je izredno pomemben faktor tudi kvaliteta podatkov. Točnost in popolnost podatkov imata lahko zelo velik vpliv na kakovost izdanih opozoril s strani rešitve za preprečevanje pranja denarja in financiranja terorizma. Pogosto se dogaja, da se podatke ročno ali tudi elektronsko dopolnjuje in spreminja (dodajanje kod, spreminjanje podatkov zaradi sprememb v procesih). Slednje lahko povzroči, da se zaradi napak ob teh dopolnitvah sprememb lahko pojavijo težave v rešitvi za PPDFT, ki se pokažejo v nepravilno izdanih opozorilih in zadetkih ali kar je še huje, da se zaradi tega kakšni zadetki ne bi ustavili oziroma sprožili generiranja opozoril. V tem primeru bi lahko bile tudi sumljive transakcije uspešno obdelane, kar izpostavi banko tveganju ugleda in morebitnim kazenskim sankcijam. Iz tega vidika je ključno, da ima banka za ustrezno delovanje rešitve za PPDFT zagotovljeno kvaliteto podatkov, ki se v ta sistem pošiljajo (PWC, 2010).

Zakonodaja zahteva od finančnih institucij, da vzpostavijo ustrezne informacijske sisteme, ki bodo preprečevali pranje denarja in financiranje terorizma. Z obzirom na vedno bolj kompleksne bančne produkte in povečevanja elektronskih plačil je zadovoljivo raven preverjanja možno doseči samo z ustreznimi tehničnimi rešitvami. Za ta namen je treba implementirati rešitve, ki predstavnikom za področje pranja denarja in financiranja terorizma omogočajo pregled in kontrolo vseh transakcij z različnimi metodami za ugotavljanje sumljivih aktivnosti.

Pri tem poznamo dva pristopa (FICO Tonbeller, 2016):

1. Pristop s postavljanjem pravil;
2. pristop s »self-learning« rešitvami.

- **Pristop s postavljanjem pravil (scenarijev)**

Te rešitve omogočajo predstavnikom preprečevanja pranja denarja in financiranja terorizma v finančni instituciji možnost opisa vedenjskih vzorcev, ki so jih zaznali v preteklosti. Kršitve nastavljenih pravil (dvigi gotovine nad določenim zneskom, pologi gotovine v velikih zneskih na novo odprte račune ...) se v obliki poročila izpišejo predstavnikom preprečevanja pranja denarja in financiranja terorizma, slednji pa morajo presoditi in po potrebi še dodatno preveriti sumljive aktivnosti. Pomanjkljivost te metode je v tem, da je treba po pripravi poročila s seznamom sumljivih plačil ročno preveriti vse podrobnosti in se ukvarjati z velikim številom neupravičeno vključenih plačil (FICO Tonbeller, 2016).

- **Pristop s »self-learning« rešitvami**

Te rešitve uporabljajo moderne tehnologije (podatkovno rudarjenje), da ustvarijo dinamične profile za vse stranke glede na njihove aktivnosti, ki so jih opravili v tej finančni instituciji v preteklosti. Na ta način bo rešitev zaznala odstopanja od običajnega vedenja in/ali ugotovil, da je določeno vedenje podobno vzorcu, ki se je pri drugih strankah izkazal kot način za pranje denarja ali financiranje terorizma. Pomanjkljivosti teh rešitev so v njihovi veliki kompleksnosti in dolgih časih implementacije (FICO Tonbeller, 2016).

Pri pristopu s postavljanjem pravil ali scenarijev je zelo pomembno, da nam rešitev omogoča čim večjo fleksibilnost. To pomeni, da lahko nastavljamo pravila za najrazličnejše vrste podatkov ali kombinacij le-teh. Dobra podpora zagotavlja tudi napredno uporabo filtrov, s katerimi se omogoči, da so kot sumljivi prikazani res relevantni zadetki. Za uporabnike je ključno tudi, da ima rešitev prijazen vmesnik, preko katerega lahko čim več teh scenarijev, brez nekega poglobljenega informacijskega znanja, vzpostavijo in spreminjajo sami (ORACLE, 2010).

4.4 Kriteriji pri izbiri rešitve za področje PPDFT

V tem poglavju so predstavljeni kriteriji, ki jih je priporočljivo upoštevati pri izbiri rešitve za preprečevanje pranja denarja in financiranje terorizma. Kriteriji so bili pripravljeni in ovrednoteni v treh fazah:

- Faza 1 - Nabor kriterijev iz literature in lastnih izkušenj.
- Faza 2 - Predlog opredelitve kriterijev (lastno ovrednotenje uteži).
- Faza 3 - Končna opredelitev kriterijev (usklajeno ovrednotenje uteži po poglobljenih intervjujih s strokovnjaki).

V prvi fazi sem iz različnih virov poiskal kriterije, ki se uporabljajo pri izbiri rešitev za preprečevanje pranja denarja in financiranje terorizma. Tem kriterijem sem dodal tudi lastne kriterije, ki se ob tovrstnih izbirah v večini primerov upoštevajo, pri čemer sem izhajal iz dosedanjih izkušenj dela v banki.

V drugi fazi sem pripravil opredelitev uteži za kriterije, ki sem jih ovrednotil na podlagi lastnih izkušenj iz poznavanja informacijskih sistemov in sistemov za preprečevanje pranja denarja in financiranja terorizma.

V tretji fazi pa sem s pomočjo poglobljenega intervjuja z vodjo področja skladnosti poslovanja in s pooblaščenko za preprečevanje pranja denarja in financiranja terorizma vse kriterije uskladil in jim v skladu z dogovorom z obema strokovnjakoma dodelil končne vrednosti za uteži.

Za metodo uporabe poglobljenega intervjuja sem se odločil, ker sem na ta način prišel do željenih podatkov. Poglobljeni intervju (Mediana, 2016), kot ena izmed metod kvalitativnega raziskovanja, namreč:

- poteka v obliki sproščenega pogovora o vnaprej določenih temah,
- je dovolj odprt, da respondentu omogoča osebno izražanje mnenj in izkušenj in
- se uporablja takrat ko želimo pridobiti mnenje strokovnjaka glede določene teme.

4.4.1 Faza 1 - Nabor kriterijev iz literature in lastnih izkušenj

V Tabeli 2 predstavljam kriterije, ki sem ji pripravil na podlagi proučene literature in lastnih izkušenj. Ob kriterijih sem opredelil vir iz katerega sem črpal podatke. Za tiste kriterije, ki sem jih dodal na podlagi lastnih izkušenj pa sem pripisal oznako: lasten vir.

Tabela 2: Nabor kriterijev iz literature in lastnih izkušenj

Kriterij	**Vir**
Cena nakupa rešitve	Protivity (2013)
Cena licenc	Lasten vir
Cena rednega vzdrževanja	Lasten vir
Garancijska doba programske rešitve	Lasten vir
Načini uvoza podatkov	Oracle (2010)
Možnost rudarjenja po podatkih	Oracle (2010)
Rešitev za zaznavo sumljivih aktivnosti	Oracle (2010)
Rešitev za pošiljanje opozoril	Oracle (2010)

se nadaljuje

Tabela 2: Nabor kriterijev iz literature in lastnih izkušenj (nad.)

Rešitev za obdelavo zadetkov	Oracle (2010)
Rešitev za pripravo poročil	Oracle (2010)
Rešitev za upravljanje s podatki	Oracle (2010)
Rešitev za upravljanje z dokumentacijo in revizijsko sledjo	Oracle (2010)
Skalabilnost rešitve	Protivity 2013
Ponudnik rešitve je zanesljiv in kredibilen partner	Lasten vir
Ponudnik rešitve ima znanje s področja preprečevanje pranja denarja	Lasten vir
Ponudnik rešitve ima znanje iz področja postavljanja pravil (scenarijev)	Protivity (2013)
Ponudnik rešitve zagotavlja dobro odzivnost	Lasten vir
Ostalo (rešitev v okviru skupine,…)	Lasten vir

Vir: ORACLE, Best practises for AML system selection and implementation, 2010; Protivity. Risk and Business Consulting. Internal Audit. *Factors to consider When Selecting an AML Transaction Monitoring System, 2013.*

4.4.2 Faza 2 - Predlog opredelitve kriterijev

V drugi fazi sem na podlagi prebrane literature in večletnih izkušenj pri izbiri programskih rešitev v banki, pripravil predlog opredelitve kriterijev. V tej fazi sem vsakemu kriteriju določil še razpon za uvrstitev in utež. Dodatno sem, z namenom boljše preglednosti tabele, uvedel še kategorije in kriterije smiselno razporedil vanje.

V tabeli so prikazani naslednji podatki:

- Kategorija
  - Omogoča, da so podobni kriteriji združeni v skupno kategorijo.
- Kriterij
  - Prikazuje seznam kriterijev, ki so bili pripravljeni v prvi fazi.
- Uvrstitev
  - Opredeljuje vrednost, ki jo doseže določena rešitev napram ostalim rešitvam. Tukaj razporedimo rešitve od najboljše do najslabše (na primer po ceni) in v tem primeru pripišemo vrednosti od 0 do 3 (0 pomeni najslabša, 3 najboljša). V primeru enostavnejših parametrov pa se vrednost določi na podlagi tega ali rešitev podpira zahteve iz kriterija ali ne in se pripiše vrednot od 0 do 1 (0 – zahteva ni podprta, 1 – zahteva je podprta).
- Utež
  - Vrednost za utež predstavlja pomembnost posameznega kriterija in zajema vrednosti od 1 do 3 (1 pomeni najmanj pomembna, 3 najbolj pomembna).

Tabela 3: Predlog opredelitve kriterijev

Kategorija	Kriterij	Uvrstitev	Utež
Splošno	Cena nakupa rešitve	0-3	3
	Cena licenc	0-3	3
	Cena rednega vzdrževanja	0-3	2
	Garancijska doba programske rešitve	0-3	1
Produkt	Načini uvoza podatkov	0-1	2
	Možnost rudarjenja po podatkih	0-1	2
	Rešitev za zaznavo sumljivih aktivnosti	0-1	3
	Rešitev za pošiljanje opozoril	0-1	1
	Rešitev za obdelavo zadetkov	0-1	1
	Rešitev za pripravo poročil	0-1	1
	Rešitev za upravljanje s podatki	0-1	1
	Rešitev za upravljanje z dokumentacijo in revizijsko sledjo	0-1	3
	Skalabilnost rešitve	0-1	3
Ponudnik rešitve	Ponudnik rešitve je zanesljiv in kredibilen partner	0-3	3
	Ponudnik rešitve ima znanje s področja preprečevanje pranja denarja	0-1	2
	Ponudnik rešitve ima znanje iz področja postavljanja pravil (scenarijev)	0-1	1
	Ponudnik rešitve zagotavlja dobro odzivnost	0-1	2
	Ostalo (rešitev v okviru skupine,…)	0-1	3

4.4.3 Faza 3 - Končna opredelitev kriterijev

V zadnji fazi sem izvedel poglobljene intervjuje z dvema strokovnjakoma, ki imata oba večletne izkušnje s področja preprečevanja pranja denarja in financiranja terorizma. Na intervjuju smo vsak kriterij pogledali, ga vsebinsko opredelili in sprejeli odločitev glede razpona in uteži. Za vsak kriterij je v stolpcu »utež«, navedena vrednost, ki predstavlja pomembnost kriterija, medtem ko stolpec »uvrstitev« vključuje vrednost, ki jo banka pripiše

rešitvam na podlagi ustrezanja kriteriju in razvrstitve v primerjavi z ostalimi rešitvami (na primer: od najboljše do najslabše po izbranem kriteriju).

Spodaj je prikazana tabela s končnimi usklajenimi vrednostmi za razpon uvrstitve in uteži, ki predstavlja pomembnost kriterija. Pod tabelo pa se nahaja sama vsebina in opredelitev kriterijev ter ključni poudarki, ki so bili izpostavljeni v okviru intervjuja. V veliki večini kriterijev je bila ocena, ki sem jo predlagal po pogovoru z obema strokovnjakoma ustrezna. Pri štirih kriterijih pa so se naše ocene razhajale, zato smo na podlagi argumentacij prišli do usklajene končne vrednosti. Ti štirje kriteriji so bili: skalabilnost rešitve, rešitev za pripravo poročil, rešitev za obdelavo zadetkov in možnost rudarjenja po podatkih.

Tabela 4: Končna opredelitev kriterijev

Kategorija	**Kriterij**	**Uvrstitev**	**Utež**
Splošno	Cena nakupa rešitve	0-3	3
	Cena licenc	0-3	3
	Cena rednega vzdrževanja	0-3	2
	Garancijska doba programske rešitve	0-3	1
Produkt	Načini uvoza podatkov	0-1	2
	Možnost rudarjenja po podatkih	0-1	1
	Rešitev za zaznavo sumljivih aktivnosti	0-1	3
	Rešitev za pošiljanje opozoril	0-1	1
	Rešitev za obdelavo zadetkov	0-1	2
	Rešitev za pripravo poročil	0-1	2
	Rešitev za upravljanje s podatki	0-1	1
	Rešitev za upravljanje z dokumentacijo in revizijsko sledjo	0-1	3
	Skalabilnost rešitve	0-1	2
Ponudnik rešitve	Ponudnik rešitve je zanesljiv in kredibilen partner	0-3	3
	Ponudnik rešitve ima znanje s področja preprečevanje pranja denarja	0-1	2
	Ponudnik rešitve ima znanje iz področja postavljanja pravil (scenarijev)	0-1	1
	Ponudnik rešitve zagotavlja dobro odzivnost	0-1	2
	Ostalo (rešitev v okviru skupine,…)	0-1	3

- ***Cena nakupa rešitve***

Ta kriterij ima v okolju, v katerem trenutno delujejo banke, zelo veliko težo, saj se slednje soočajo z velikimi pritiski na stroške in so primorane izbirati optimalne rešitve. Pri izbiri rešitve za preprečevanje pranja denarja to pomeni, da morajo izbrati rešitve, ki za svojo ceno v kar največji meri pokrijejo vse zahteve, ki izhajajo iz zakonodajnih okvirov in internih pravil. Nezanemarljivo dejstvo pri tem je, da zakon nalaga enake naloge in zahteve majhnim in velikim bankam, kar pomeni še dodatni pritisk na manjše banke, ki zaradi manjših volumnov težje kupijo dražje in učinkovitejše rešitve.

Pri tem kriteriju se pod uvrstitev zavede tri najugodnejše rešitve (najugodnejša s številko 3, najmanj ugodna s številko 1). Če izbiramo med več kot tremi rešitvami, ima vsaka naslednja pod uvrstitev zavedeno stopnjo 0. Ker uvedba rešitve za PPDFT predstavlja precejšen odhodek za banko, je utež postavljena zelo visoko na stopnjo 3 (na tristopenjski lestvici).

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Argument za določene vrednosti je bil padanje prihodkov bank, s katerim se sooča celoten bančni sektor.

- ***Cena licenc***

Cena licenc vpliva na stroške banke, zato je utež prav tako postavljena na stopnjo 3. Pri licencah je treba paziti, da pokriva vse rešitve, ki jih vpeljujemo, saj ponudniki rešitev za PPDFT-licence največkrat vežejo na posamezne module, ki jih rešitev ponuja. Zelo pomembno je tudi trajanje veljavnosti licenc, ki so običajno omejene na eno leto. Ključno je, da ob primerjavi preverimo tudi, da licence zajemajo oziroma pokrivajo enake storitve (uporaba rešitve, redne nadgradnje, dostop do ponudnika rešitve).

Pri tem kriteriju se pod uvrstitev zavede tri najugodneje rešitve (najugodnejša s številko 3, najmanj ugodna s številko 1). Če analiziramo več rešitev, ima vsaka naslednja pod uvrstitev zavedeno stopnjo 0. Ker licence v večini primerov predstavljajo precejšen odhodek za banko, je utež postavljena zelo visoko na stopnjo 3 (na tristopenjski lestvici).

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Izpostavljen je bil predlog, da se s ponudnikom dobro preveri povezanost licenc z določenimi moduli oziroma funkcionalnostmi, saj je ob začetni implementaciji zaradi večjega paketa mogoče dogovoriti ugodnejše pogoje za licence. Glede vrednosti za utež in uvrstitev je bilo doseženo strinjanje na podlagi argumenta padanja prihodkov bank.

- ***Cena rednega vzdrževanja***

Ta kriterij je prav tako eden izmed ključnih za dolgoročno partnerstvo med banko in ponudnikom rešitve, saj predstavlja neko kontinuirano vez pri nakupu rešitve. Ker prav

tako vpliva na stroške banke, ima utež postavljeno na stopnjo 2. Banka mora biti pri dogovoru o ceni rednega vzdrževanja pozorna, da si zagotovi ustrezno podporo s strani ponudnika za primere izpadov. Na tej točki je treba imeti zelo podrobno opredeljen razpon nalog, ki se bodo izvajale v okviru vzdrževanja in ure, v katerih je ponudnik na voljo za reševanje težav.

Na ta način lahko pripravimo razvrstitev, kateri izmed ponudnikov največ ponuja in jih ponovno razvrstimo od prvega do tretjega mesta. Ponudniku, ki nudi najnižjo ceno v okviru rednega vzdrževanja s primerljivim naborom storitev, pripišemo stopnjo uvrstitve 3, naslednjemu 2 in tretjemu v razvrstitvi 1. Če analiziramo več rešitev, ima vsaka naslednja pod uvrstitev zavedeno stopnjo 0. Za ceno rednega vzdrževanja je utež glede na pomembnost pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Glede vrednosti za utež in uvrstitev je bilo doseženo strinjanje na podlagi argumenta padanja prihodkov bank.

- ***Garancijska doba izbrane rešitve***

V garancijski dobi ponudnik rešitve ponuja odpravo napak. Iz tega vidika je pomembno, da je doba čim daljša, saj je za identifikacijo določenih napak včasih potrebno kar nekaj časa. Pri tem gre predvsem za kakšna pravila, ki so namenjena temu, da identificirajo sumljivo poslovanje v nekem daljšem časovnem obdobju. Zato se pri tem kriteriju upošteva dolžina trajanja garancije hkrati pa je potrebno biti pozoren, da pod pojem garancije ponudniki zavedejo primerljive storitve.

Pri tem kriteriju se pod uvrstitev zavede tri ponudnike z najdaljšo garancijsko dobo (najdaljša doba s številko 3, najkrajša doba izmed prvih treh pa s številko 1). Če analiziramo več rešitev, ima vsaka naslednja pod uvrstitev zavedeno stopnjo 0. Če bi se zgodilo, da imata prvouvrščeni rešitvi enako garancijsko dobo, se obema pripiše stopnja uvrstitve 3, preostali rešitvi pa stopnja 2. Vedno pa so po stopnji lahko označene samo tri najboljše rešitve. Vsaka rešitev, uvrščena od 3. mesta navzgor, ima pripisano stopnjo 0. Za garancijsko dobo je utež glede na pomembnost pri izbiri rešitve postavljena na stopnjo 1.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. S strani pooblaščenke za pranje denarja je bilo izpostavljeno, da mora dolžina garancijske dobe trajati toliko časa, da se preveri pravilnost vseh scenarijev. Običajno so scenariji, ki spremljajo daljše časovno obdobje vezani na obdobje enega leta. Glede vrednosti za utež in uvrstitev je bilo doseženo strinjanje na podlagi argumenta, da se mora zagotoviti pravilnost delovanja vseh scenarijev.

- ***Načini uvoza podatkov***

Pri načinih uvozov podatkov sta pomembni dve stvari:

1. Rešitev mora omogočati takojšnjo neposredno komunikacijo preko spletnih servisov, kot tudi možnosti uvozov podatkov preko datotek;
2. rešitev mora omogočati uvoze v različnih formatih. Zaradi avtomatizacije in digitalizacije vedno bolj v ospredje prihajajo rešitve, ki omogočajo takojšnjo neposredno komunikacijo, saj takoj vrnejo rezultate in tako omogočajo pohitritve postopkov. Za obdelavo večje količine podatkov ali preverjanje celotnih portfeljev strank pa so še vedno pomembni uvozi teh podatkov preko datotek, ki se lahko izvajajo tudi izven delovnih časov bank.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če rešitev ponuja možnost uvoza, ki je navedena tako pod točke 1 kot tudi 2 iz odstavka zgoraj. Če katera izmed teh zahtev ni podprta, se rešitvi pripiše stopnja 0. Za način uvoza podatkov je utež glede na pomembnost pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Izpostavljena je bila možnost uvoza različnih datotek saj se s tem izognemo večjim razvojem v obstoječih sistemih, ki bodo vir za pripravo podatkov. Glede vrednosti za utež in uvrstitev je bilo doseženo strinjanje na podlagi argumenta, da rešitev omogoča čim boljšo in enostavnejšo povezljivost z obstoječimi rešitvami, ki jih banka uporablja.

- ***Možnost rudarjenja po podatkih***

S povečevanjem števila informacij in podatkov, ki jih banke zbirajo o svojih strankah, se povečujejo tudi možnosti napredne obdelave teh podatkov in iskanja vzorcev obnašanj, ki jih stranke zasledujejo. V preteklosti je zadostovalo, če so banke spremljale samo določen kritičen produkt, ki je bil bolj izpostavljen tveganju. V današnjem času pa je, tudi zaradi prilagodljivosti oseb, ki se ukvarjajo s pranjem denarja ali financiranjem terorizma, treba uporabiti napredne metode, ki omogočajo preverjanje informacij iz različnih poslovnih enot, različnih bančnih računov in tudi različnih bančnih produktov. S tega vidika je pomembno, če imamo za odkrivanje teh vzorcev na voljo tudi možnost rudarjenja po podatkih.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če rešitev ponuja možnost rudarjenja po podatkih. Če rešitev tega ne podpira, se pripiše stopnja 0. Za možnost rudarjenja po podatkih je pomembnost pri izbiri rešitve postavljena na stopnjo 1.

Ključni poudarki iz poglobljenega intervjuja:
Pri tem kriteriju smo imeli za vrednost uteži različno mnenje. Osebno sem zagovarjal višjo vrednost za utež, medtem ko je pooblaščenka zagovarjala nižjo vrednost za utež pri tem kriteriju. Na koncu smo na podlagi argumenta, da je trenutno za uporabo teh metod potrebno

posebno strokovno znanje in zelo dolg čas, kriteriju pripisali nižjo vrednost. Potrebno pa je upoštevati, da bo v prihodnosti ta kriterij lahko postal bolj relevanten.

- ***Rešitev za zaznavo sumljivih aktivnosti***

Rešitev za PPDFT mora zaznati vsako sumljivo aktivnost, kar pomeni, da mora nenehno spremljati aktivnosti bančnih strank preko transakcij, računov ali uporabe ostalih bančnih produktov. Pri tem je zelo pomembno, da so zadetki, ki jih odkrije rešitev, kar se da točni in da se osebe, ki so pooblaščene v bankah za pranje denarja, ne ukvarjajo z nepravilnimi zadetki. Prav tako je pomembno, da rešitev omogoča prikaz čim večjega števila podatkov o samem zadetku že znotraj same rešitve. Iz tega naslova se od rešitve pod tem kriterijem pričakuje zmožnost učinkovite spremljave aktivnosti bančnih strank in zagotavljanja kar se da točnih zadetkov v primeru odkritja sumljivih transakcij. Sledenje je možno doseči z nastavitvijo pravil, s katerimi bo rešitev te sumljive aktivnosti identificirala in ravno prilagodljivost in tehnološka naprednost pri postavljanju teh pravil odlikuje najboljše rešitve za PPDFT.

Pri tem kriteriju se pod uvrstitev zavede tri rešitve, ki ponujajo najboljšo možnost upravljanja pravil za identifikacijo sumljivih aktivnosti (najboljša rešitev dobi stopnjo številka 3, naslednja dobi stopnjo 2 in še naslednja stopnjo 1). Če analiziramo več rešitev, ima vsaka naslednja pod uvrstitev zavedeno stopnjo 0. Ker je to ključna funkcionalnost rešitve za PPDFT, je utež postavljena zelo visoko na stopnjo 3 (na tristopenjski lestvici).

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Pri tem kriteriju je šlo za ključno funkcionalnost rešitve za preprečevanje pranja denarja in financiranja terorizma zato je bila zelo hitro potrjena visoka vrednost za utež. Ob tem je bilo še izpostavljeno, da mora rešitev zagotavljati uporabniku prijazen vmesnik za spreminjanje scenarijev in pravil, ki ga lahko uporabljajo tudi pooblaščenci za pranje denarja, ki običajno nimajo posebnih znanj iz IT področja.

- ***Rešitev za pošiljanje opozoril***

Procesi pri upravljanju področja PPDFT v banki so velikokrat prepleteni med različnimi oddelki. Vključeni so tako zaposleni iz prodaje, ki delujejo v poslovalnicah, zaposleni iz zaledja, ki se ukvarjajo z odpiranjem strank in računov, v zelo veliki meri so vključeni zaposleni, ki skrbijo za procesiranje plačilnih transakcij, in ne nazadnje so tukaj še zaposleni, ki so pooblaščenci za pranje denarja v bankah. Zaradi velikega števila vključenih ljudi in enot je nujno poskrbeti za dobro obveščenost vseh udeležencev, kar omogoči vzpostavitev učinkovitih procesov. Zaradi tega mora rešitev omogočati avtomatizirano obveščanje na podlagi določenih pravil in kar je mogoče še pomembneje, omogočiti mora, da ustrezna obvestila prejmejo ustrezni oddelki ali ljudje. Vse to je mogoče, če je rešitev za obveščanje pripravljena dovolj fleksibilno in z možnostjo prilagajanja zahtevam naročnika, v našem primeru banke.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če rešitev ponuja možnost fleksibilnega pošiljanja sporočil. Če rešitev tega ne podpira, se pripiše stopnja 0. Za pošiljanja sporočil je utež pri izbiri rešitve postavljena na stopnjo 1.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Izpostavljena je bila možnost neposrednega naslavljanja zahtevkov na skrbnike posameznih strank. Trenutno večina rešitev omogoča obveščanje preko internih list z elektronskimi naslovi, kar pa je manj učinkovito.

- ***Rešitev za obdelavo zadetkov***

Pri tem kriteriju je najpomembneje, da ima uporabnik na voljo prijazen vmesnik, ki mu omogoča pregled zadetkov in prikaz čim večjega števila informacij o samem zadetku na enem mestu. To je ključno z vidika lažjega in hitrejšega odločanja o nadaljnjih postopkih, ki morajo biti izvedeni v primeru zadetka. Rešitev mora uporabniku omogočati, da si naredi pregleden prikaz nalog, ki ga čakajo. Zelo uporaben in učinkovit mora biti tudi iskalnik že obdelanih zahtevkov. Ker se ta rešitev uporablja vsakodnevno in za zelo odgovorne naloge, kot so spremljave sumljivih aktivnosti s področja PPDFT, imajo zelo velik vpliv tudi na zadovoljstvo zaposlenih, ki jo uporabljajo. Predpogoj, da slednji dobro opravljajo svoje delo je, da so na delovnem mestu zadovolji, kar vključuje tudi uporabo ustreznih rešitev.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1,če rešitev nudi uporabniku prijazno in učinkovito izkušnjo pri obdelavi zahtevkov. Če rešitev tega ne podpira, se pripiše stopnja 0. Za rešitev za obdelavo zadetkov je utež pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Pri rešitvi za obdelavo zadetkov se nismo strinjali pri oceni uteži. Medtem ko sem sam zagovarjal nižjo utež, sta oba kolega izpostavila, da je ta funkcionalnost ključna pri učinkovitem boju proti tveganjem iz naslova PPDFT. Poseben poudarek je na hitrosti obdelave zadetkov, zato mora rešitev ponuditi uporabniku čim več informacij in mu omogočiti hitro izpeljavo procesa (prikaz vzroka za sumljivost transakcije, priprava in posredovanje poročil pristojnim organom). Na podlagi te argumentacije smo to utež zvišali iz vrednosti 1 na vrednost 2.

- ***Rešitev za pripravo poročil***

Ker je področje PPDFT postalo v preteklih letih vedno bolj izpostavljeno in ker je zakonodaja z vidika neposredne odgovornosti za to področje vključila člane uprav bank, se je pritisk na pripravo raznih poročil zelo povečal. Rešitev mora zagotavljati pripravo poročil tako za zunanje akterje (primer: Urad za preprečevanje pranja denarja, sodišča …), kot tudi za interne uporabnike (predsednike uprav, notranje revizorje …). Ker količina in kompleksnost produktov naraščata, mora rešitev zagotavljati prilagodljive vmesnike s

pomočjo katerih si lahko uporabniki, brez poglobljenega tehničnega znanja z vidika pisanja poizvedb, pripravijo želene podatke in jih predajo naročnikom v pregled. Ker se na podlagi teh poročil sprejemajo odločitve tudi na najvišjih ravneh v bankah, je ta kriterij precej pomemben.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1,če rešitev nudi uporabniku prijazno in učinkovito možnost priprave poročil. Če rešitev tega ne podpira, se pripiše stopnja 0. Za rešitev za pripravo poročil je utež pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Pri rešitvi za pripravo poročil se prav tako nismo strinjali glede vrednosti uteži. Medtem ko sem jaz zagovarjal nižjo utež, sta kolega zagovarjala višjo utež. Dogovor smo dosegli na podlagi argumentacije o višini glob, ki je zagrožena za banko in njeno upravo v primeru kršitev določil zakona o PPDFT. Ker morajo odločevalci imeti točne in promptne informacije za svoje odločanje, je dobra rešitev za pripravo poročil ključna in tako smo rešitvi dodelili utež z vrednostjo 2, medtem ko je bil moj predlog, da bi bila ta vrednost 1.

- ***Rešitev za upravljanje s podatki***

Ključno kar mora rešitev za upravljanje s podatki pokrivati je možnost izvajanja različnih kontrol z vidika kvalitete podatkov. Zelo pogosto se veliko pozornosti usmerja količini podatkov, ki se jih potrebuje, a se pri tem zanemari kvaliteta podatkov. Če želimo učinkovito rešitev, ki bo javljala pravilne zadetke, potem morajo biti podatki v prvi vrsti na voljo, hkrati pa tudi popolnoma pravilni. Zato mora rešitev za upravljanje s podatki vsebovati možnost vzpostavljanja kontrol in preverjanja kvalitete podatkov, ki se obdelujejo v rešitvi za PPDFT.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če rešitev nudi uporabniku možnost vzpostavitve kontrol, ki omogočajo zagotavljanje pravilnosti podatkov. Če rešitev tega ne podpira, se pripiše stopnja 0. Za kriterij rešitve za upravljanje podatkov je utež pri izbiri rešitve postavljena na stopnjo 1.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Izpostavljeno je bilo, da bi za kvaliteto podatkov bilo potrebno poskrbeti že v sistemih, ki pošiljajo podatke v rešitev za PPDFT. Kljub temu smo kriterij vključili z vrednostjo 1, ob argumentaciji, da je za kakovost podatkov potrebno skrbeti v vseh delih banke.

- ***Rešitev za upravljanje z dokumentacijo in revizijsko sledjo***

Za ustrezno pokrivanje področja PPDFT v banki veljajo strogi zakoni in v primeru odkritih sumljivih aktivnosti je treba vse postopke izpeljati zelo strokovno in profesionalno, da se lahko potem v nadaljnjih postopkih na sodiščih, dokaže dejanske zlorabe. Ob tem so banke dolžne dokazati, da so z ustreznim upravljanjem dokumentacije izvajale vse postopke v

skladu z zahtevami regulatorjev. Zato mora rešitev omogočati hrambo in upravljanje vse dokumentacije, povezane s področjem preprečevanja pranja denarja in financiranja terorizma ali zagotavljati ustrezno povezljivost z bančnim dokumentnim sistemom za arhiviranje dokumentacije. Dodatno mora rešitev beležiti kdo, kdaj in kaj je za potrebe preprečevanja pranja denarja in financiranja terorizma v banki naredil kakršnekoli vpoglede, spremembe, zavrnitve ali potrditve tako na strankah kot tudi na sistemskih nastavitvah (primer: sprememba pravila za odkrivanje sumljivih transakcij …).

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če rešitev nudi uporabniku možnost upravljanja z dokumentacijo in beleženje revizijske sledi. Če rešitev tega ne podpira, se pripiše stopnja 0. Za kriterij rešitve za upravljanje z dokumentacijo in revizijsko sledjo je utež pri izbiri rešitve postavljena na stopnjo 3.

Ključni poudarki iz poglobljenega intervjuja:
Pri rešitvi za upravljanje z dokumentacijo in revizijsko sledjo se prav tako nismo strinjali glede vrednosti uteži. Osebno sem tukaj zagovarjal nižjo utež, medtem ko je vodja oddelka skladnosti poslovanja zagovarjal visoko utež. Na podlagi argumentacije, da v primeru morebitnih pomanjkljivosti pri tej rešitvi morebiti ne bi bili sposobni dokazati krivde nekoga, ki je preko banke pral denar, smo se uskladili, da je tej rešitvi potrebno posvetiti zelo veliko pozornosti. Na podlagi tega smo ji pripisali najvišjo možno utež.

- ***Skalabilnost rešitve***

Banka mora ob nakupu PPDFT-rešitve predvidevati svojo nadaljnjo rast ali morebitne združitve z drugimi bankami ali hranilnicami, saj ima vsaka rešitev omejitve glede količine podatkov, ki jih lahko obdela. Pri tem pride do izraza možnost rešitve po skalabilnosti, kar pomeni, da jo je moč razširiti ali dograjevati na način, da bo sposobna obdelave tudi večjih količin podatkov.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če rešitev je skalabilna. Če rešitev ni skalabilna, se pripiše stopnja 0. Za kriterij skalabilnosti rešitve je utež pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Tudi pri skalabilnosti rešitve smo se dalj časa usklajevali glede uteži. Medtem ko sem jaz zagovarjal najvišjo možno utež, sta kolega zagovarjala najnižjo utež. Po argumentaciji z moje strani o podobnih težavah, ki so se že pojavljale, tako pri nas kot tudi pri drugih bankah, smo se dogovorili, da naredimo kompromisno rešitev in skalabilnosti pripišemo za utež vrednost 2.

- ***Ponudnik rešitve je zanesljiv in kredibilen partner***

Ker gre v primeru nakupa rešitve za preprečevanje pranja denarja in financiranja terorizma za strateško odločitev banke, mora tudi izbira ponudnika biti dobro premišljena. Kot

ključno zahtevo morajo banke tukaj upoštevati reference ponudnika rešitve. Vsekakor se pričakuje, da je ponudnik vzpostavil rešitev pri vsaj petih bankah ali drugih finančnih institucijah. Zelo priporočljivo je tudi, da si banka rešitev pri eni izmed bank, ki so jo že postavile tudi ogleda in se ob tem pogovori o kredibilnosti priporočil ponudnika rešitev. Glede same zanesljivosti in stabilnosti ponudnika pa se preveri, kako uspešno posluje in kako dolgo že deluje na trgu s svojimi rešitvami za preprečevanje pranja denarja in financiranja terorizma. Glede samega poslovanja se pričakuje, da je zadnjih pet let podjetje poslovalo z dobičkom. Glede prisotnosti na trgu pa je minimalno obdobje 10 let.

Pri tem kriteriju se pod uvrstitev zavede tri rešitve, ki ponujajo najboljše reference in zanesljivost delovanja. Predpogoj za uvrstitev med prve tri so pozitivni poslovni rezultati zadnjih 5 let in vsaj 10 letna prisotnost na trgu. Razvrstitev po prvih treh pa se izvede na podlagi števila referenc za rešitev preprečevanja pranja denarja in financiranja terorizma, ki jih ponudnik lahko navede (tisti z največ referencami ima stopnjo številka 3, naslednja potem dobi stopnjo 2 in še naslednja stopnjo 1). Če analiziramo več rešitev, ima vsaka naslednja pod uvrstitev zavedeno stopnjo 0. Ker je to ključni kriterij, ki zagotavlja dolgoročno stabilnost ponudnika rešitve za preprečevanje pranja denarja in financiranja terorizma, je utež postavljena zelo visoko na stopnjo 3 (na tristopenjski lestvici).

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. S strani pooblaščenke za PPDFT je bilo izpostavljeno, da je zelo priporočljivo, če ponudnik že ponuja rešitve na trgu v katerem banka deluje, saj ima vsak trg kljub precej poenoteni mednarodni zakonodaji, svoje posebnosti. Glede vrednosti za utež in uvrstitev smo se strinjali, da je kredibilnost ponudnika rešitve ključna, kar je hkrati bil tudi argument za dodelitev najvišje uteži.

- ***Ponudnik rešitve ima znanje s področja preprečevanja pranja denarja***

Za pokrivanje tako zahtevnega področja kot je razvoj rešitev za področje preprečevanje pranja denarja je nujno, da ima ponudnik rešitve tudi interno znanje s tega področja in da sprotno spremlja razvoj in nadgrajuje svoje rešitve. Zaradi kompleksnosti zakonodajnih zahtev je nujno, da ima ponudnik dovolj strokovno podkovan kader, da lahko razume in implementira vse zahteve v svoje programe. Ker so ponudniki specializirani za te rešitve, se v sklopu tega pričakuje, da lahko bankam tudi svetujejo pri reševanju težav ob uvedbi rešitve. Ob tem je treba izpostaviti, da se od ponudnika pričakuje tako tehnično znanje, ki je potrebno, da se rešitev vzpostavi znotraj tehnične bančne infrastrukture, kot tudi vsebinskega znanja, ki je potrebno za obdelavo podatkov in pripravo različnih pravil za spremljavo sumljivih aktivnosti v banki. Če ima ponudnik tudi znanje o nacionalnih posebnostih, ki se v vsaki državi pojavljajo ob sprejemanju ZPPDFT, predstavlja to še dodaten plus.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če smo pri referencah dobili potrditev, da so kadri ponudnika ustrezno usposobljeni in premorejo dovolj vsebinskega znanja s področja preprečevanja pranja denarja in financiranja terorizma. Če te potrditve pri referencah ne dobimo, se pripiše stopnja 0. Za prisotnost znanja s področja preprečevanje pranja denarja je utež pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. S strani obeh kolegov je bilo tukaj izpostavljeno, da je zelo priporočljivo, če ima ponudnik rešitve na voljo kompetentne ljudi, ki lahko pomagajo banki pri vzpostavitvi rešitve, hkrati pa tudi izvedejo prenos znanja. Argument za precej visoko utež tukaj je bil, da brez prenosa tega znanja v banko, slednja ne more učinkovito obvladovati tveganj s področja PPDFT.

- ***Ponudnik rešitve ima znanje iz področja postavljanja pravil (scenarijev)***

Dobro poznavanje podatkov, ki se uvažajo, in ustrezno postavljanje pravil za ugotavljanje sumljivih aktivnosti je ključna naloga ob uvedbi nove rešitve za preprečevanja pranja denarja. V veliko pomoč tukaj so lahko izkušnje ponudnika PPDFT-rešitve, ki se je že ob ostalih implementacijah srečal s postavitvami pravil in ki ve, katera osnovna pravila so potrebna za zadostitev zakonodajnim okvirjem. Vsekakor pa je na tem mestu znanje in pomoč ponudnika le v tej meri, da olajša delo ob uvedbi novega programa, medtem ko vsa odgovornost za pravilne nastavitve in delovanje pravil ostane na banki.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1, če smo pri referencah dobili potrditev, da ponudnik rešitev ima znanje s področja postavljanja pravil in jih ob uvedbi rešitve tudi aktivno skupaj z banko implementira. Če te potrditve pri referencah ne dobimo, se pripiše stopnja 0. Za prisotnost znanja s področja postavljanja pravil (scenarijev) je utež pri izbiri rešitve postavljena na stopnjo 1.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Pri tem kriteriju je ponudnik rešitve lahko v veliko pomoč banki. Kot je povedala pooblaščenka za PPDFT imajo tisti ponudniki, ki imajo večje število svojih rešitev že vzpostavljenih pri drugih bankah, tudi veliko izkušenj s postavitvijo scenarijev. To lahko precej olajša delo ob vzpostavitvi same rešitve. Ob argumentu, da je tukaj ponudnik rešitve lahko samo v pomoč banki, ne more pa prevzeti odgovornosti, je bila utež postavljena na vrednost 1.

- ***Ponudnik rešitve zagotavlja dobro odzivnost***

Kakovostna in hitra odzivnost ponudnika rešitve prihajata vedno bolj v ospredje zaradi neposrednih povezav preko spletnih servisov, ki v realnem času preverjajo transakcije ali podatke o stranki. Zaradi tega mora ponudnik ponujati visoko odzivnost. Pričakovanja tukaj so 30 min za prvi odziv in 4 ure za odpravo kritičnih napak. Zaradi tega mora

ponudnik zagotavljati strokovno in usposobljeno ekipo za podporo banki. Preko referenc je tudi priporočljivo preveriti, ali je ob hitri odzivnosti tudi nivo storitev ustrezen.

Pri tem kriteriju se pod uvrstitev zavede s stopnjo 1 v primeru, da je ponudnik sposoben ponuditi pogoje odzivnosti, kot so navedeni v odstavku zgoraj. Če tega ni sposoben ponuditi, se pripiše stopnja 0. Za zagotavljanje dobre odzivnosti je utež pri izbiri rešitve postavljena na stopnjo 2.

Ključni poudarki iz poglobljenega intervjuja:
Usklajena je bila vsebina kriterija in dogovor o vrednosti za utež in uvrstitev. Tukaj je bila izpostavljena precejšnja odvisnost od ponudnika v primeru težav, ker se veliko ključnih bančnih sistemov, kot so na primer plačilni sistemi ali pa sistemi za odpiranje strank, povezujejo z rešitvami za PPDFT. Iz tega naslova mora biti zagotovljena res hitra in ustrezna podpora. Slednje je bil tudi argument, da smo temu kriteriju pripisali srednje visoko utež.

- ***Ostalo***

Pod tem kriterijem se lahko zavede posamezna specifika vsake banke, ki išče rešitev za preprečevanje pranja denarja in financiranja terorizma. Kot primer se lahko tukaj uporabi, da je banka del večje bančne skupine, ki že ima rešitev za preprečevanje pranja denarja in financiranja terorizma implementirano v ostalih svojih podružnicah in želi imeti poenoteno infrastrukturo za preprečevanje pranja denarja in financiranja terorizma.

Pod kriterij ostalo se zavede samo kriterije, ki so zelo pomembni in ki morajo relevantno vplivati na odločitev za izbiro rešitve za preprečevanje pranja denarja in financiranja terorizma. Zato se pod ta kriterij zavede pod uvrstitev stopnja 3, če banka oceni, da je ta kriterij nujen. Prav tako se potem za ta kriterij utež pri izbiri rešitve postavi na stopnjo 3.

Ključni poudarki iz poglobljenega intervjuja:
Pri tem kriteriju je bilo veliko razprave o vrednosti, ki jo bomo pripisali za utež in uvrstitev. Na koncu smo se odločili, da dodamo za obe vrednosti najvišjo možno stopnjo, na banki pa leži odgovornost, da kritično oceni ali je kriterij, ki ga želi vključiti pod ostalo res tako relevanten, da nosi tako veliko utež pri odločitvi. Argumentacije tukaj je bila, da določene situacije kot je na primer ta, da banke znotraj iste skupine uporabljajo isto rešitev, zahteva uporabo posebnega kriterija z visoko stopnjo uteži.

4.4.4 Matrika za odločanje

Matrika za odločanje je sestavljena iz pomnoženih in seštetih vrednosti, ki jih dobimo za kriterije po formuli:

$$\sum = (X_1 * Y_1) + (X_2 * Y_2) + ...(X_{19} * Y_{19}) \qquad (1)$$

Rešitev, ki po tej matriki doseže največ točk, je najprimernejša rešitev za banko.

S pomočjo matrike za odločanje in uporabo navedenih kriterijev lahko banka izbere optimalno rešitev za svoje potrebe in tako zagotovi za področje tehnološke rešitve, skladnost z zahtevami iz zakona o preprečevanju pranja denarja in financiranja terorizma.

SKLEP

Sklepni del magistrske naloge odpiram z opisom iz Konvencije združenih narodov o korupciji, ki slikovito opiše, zakaj se je treba lotevati področja preprečevanja pranja denarja in financiranja terorizma z veliko odgovornostjo. Korupcija, v sklop katere sodita tudi pranje denarja in financiranje terorizma, je kot »zahrbtna bolezen, ki ima uničujoč vpliv na družbo. Spodkopava demokracijo in pravno državo, vodi v kršenje človekovih pravic, znižuje kvaliteto življenja družbe kot celote ter hkrati omogoča razcvet kriminala, terorizma in predstavlja splošno grožnjo za varnost ljudi« (Konvencija združenih narodov, 2004). Ravno ta višji cilj varnosti bi moral biti v ospredju, ko se banke lotevajo urejevanja področja preprečevanja pranja denarja in financiranja terorizma. V praksi je tisti sprožilec, ki največkrat da zagon za spremembe na tem področju, žal še vedno zakonski oziroma kazenski del, ki se izrazi v globah. Ravno zaradi tega in zaradi povečanega tveganja iz naslova terorizma, pa so v zadnjih letih v bankah in tudi pri ponudnikih, nove rešitve za preprečevanje pranja denarja izrazito izboljšale obvladovanje tega področja.

V prvem delu naloge je prikazan razvoj pranja denarja in financiranja terorizma skozi zgodovino. Ocenjujem, da ta del predstavlja zanimiv vpogled v razvoj pranja denarja in financiranja terorizma, ki je bil že v zgodovini zelo intenziven in za katerega pričakujem, da bo tudi v prihodnje bankam ponujal številne izzive. Nadalje je prikazan napredek, ki so ga mednarodne organizacije dosegle na tem področju s sprejemanjem različnih konvencij, priporočil in direktiv. Kot ključne ugotovitve tega dela izpostavljamo prikaz razvoja širjenja obsega dejanj, ki so iz kriminalnih aktivnostih, povezanih z drogami, prešle na aktivnosti, ki vključujejo in so posledice nekega predhodnega kriminalnega dejanja. Da je področje preprečevanja pranja denarja in financiranja terorizma zelo aktualno, smo dokazali tudi s prikazom višin glob izdanih v zadnjih letih, ki so se izredno povečale in ki so povzročile, da so se banke začele zelo dejavno ukvarjati s tem področjem.
V drugem delu magistrske naloge sem se poglobil še v osnutek Zakona o preprečevanju pranja denarja in financiranja terorizma ZPPDFT in naredil analizo, iz katerih členov izhajajo zahteve, ki jih pokrivamo z rešitvami za PPDFT. Slednje je predvsem pomembno za dobro razumevanje potreb, ki jim morajo zadostiti rešitve za PPDFT, in predstavlja uporabno informacijo za vse, ki želijo v strnjeni obliki videti pregled teh zahtev. Hkrati pa jim relacija s členi omogoča hitro iskanje dodatnih informacij neposredno iz zakona, če bi to bilo potrebno. Nadaljeval sem z opisom funkcionalnosti, ki jih omogočajo rešitve za

PPDFT. Slednje bralcu pomaga bolje razumeti kaj lahko pričakuje od rešitev za PPDFT in ga opremi z dodatnim znanjem za pogovore z različnimi ponudniki rešitev.

V osrednjem in hkrati poglavitnem delu magistrske naloge, pa sem pripravil kriterije in matriko, s pomočjo katere bodo banke lahko izbirale rešitve za preprečevanje pranja denarja in financiranje terorizma. Slednje sem izvedel s pomočjo analiziranja literature, posvetovanja s strokovnjaki za pranje denarja ter lastnih izkušenj. Rezultat teh aktivnosti je nabor kriterijev z opredelitvami uteži ter pripravljena matrika za odločanje. Kriterije sem podrobno opisal in jih natančno opredelil tako, da predstavljajo koristen pripomoček za banke. Ta del predstavlja raziskovalno analitsko komponento moje naloge. V tem delu vidim svoj prispevek k znanosti in upam, da se bo s pomočjo te naloge marsikatera banka odločila za najboljšo možno rešitev za preprečevanje pranja denarja in financiranja terorizma. Ocenjujem, da sem s tem uspešno dosegel cilj, ki sem si ga zadal v magistrski nalogi.

Za konec bi še enkrat izpostavil, da je poleg izbire najboljše rešitve za PPDFT za uspešno zagotavljanje skladnosti področja preprečevanja pranja denarja in financiranja terorizma ključno to, da so zagotovljeni in urejeni tudi vsi ostali dejavniki, ki vplivajo na to področje. Ti dejavniki so politika upravljanja področja, zaposleni, procesi, ustrezno urejen operativni del, zagotovljeno upravljanje tveganj in nadzora ter ne nazadnje tudi ustrezna kakovost podatkov.

Magistrska naloga je pripravljena z namenom nuditi pomoč bankam pri odločitvi za ustrezno rešitev za preprečevanje pranja denarja in financiranja terorizma.

LITERATURA IN VIRI

1. Acams Today. (b.l.). Business Model for a Terrorist Organisation. Najdeno 10. januarja 2016 na spletnem naslovu http://www.acamstoday.org/business-model-for-a-terrorist-organization/
2. Acuity. (b.l.). Trends in Anti-Money Laundering (AML) compliance. Najdeno 10. januarja 2016 na spletnem naslovu http://www.accuity.com/industry-updates/free-resources/trends-in-aml-compliance-infographic/
3. Anti Money laundering Forum. (b.l.). Europe - History of the European Union Anti-Money Laundering and Financing of Terrorism Directives. Najdeno 3. januarja 2016 na spletnem naslovu http://councilforeuropeanstudies.org/?gclid=COmqxaf5g80CFUqeGwoduWQOAw
4. Božičnik, S. (2000). Pranje denarja. V S. Stipič (ur.), *Naše gospodarstvo 46*(2/3), 453–464.
5. *Cellet Finance solutions AG.* Najdeno 16. decembra 2014 na spletnem naslovu http://www.cellent-fs.de
6. Chatain, P.-L., McDowell, J., Mousset, C., Schott, P. A., & van der Does de Willebois, E. (2009, 11. maj). Preventing money laundering and terrorist financing: A practical guide for bank supervisors. *The World Bank.* Najdeno 5. januarja 2016 na spletnem naslovu http://www.amazon.com/Preventing-Money-Laundering-Terrorist-Financing/dp/0821379127
7. Council of Europe. (b.l.a). Details of Treaty No.141. Najdeno 14. decembra 2015 na spletnem naslovu http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/141
8. Council of Europe. (b.l.b). Chart of signatures and ratifications of Treaty 198. Najdeno 14. decembra 2015 na spletnem naslovu http://www.coe.int/en/web/conventions /search-on-treaties//conventions/treaty/198/signatures?p_auth=FG nqG6KU
9. Deloitte. (b.l.). The fourth EU Anti Money laundering Directive. Najdeno 3. januarja 2016 na spletnem naslovu https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf
10. Deutsch, N. (2009, 23. julij). Kriminal belih ovratnikov. *Revija kapital.* Najdeno 20. januarja 2016 na spletnem naslovu http://www.revijakapital.com/kapital/aktualno.php?idclanka=6900
11. Direktiva evropskega parlamenta in Sveta 2001/97/ES. *Uradni list Evropskega Parlamenta š*t. 97/2001 – L 344.
12. Direktiva evropskega parlamenta in Sveta 2005/60/ES. *Uradni list Evropskega Parlamenta š*t. 60/2005 - L 309/15.
13. Direktiva evropskega parlamenta in Sveta 2015/849. *Uradni list Evropskega Parlamenta š*t. 849/2015 – L 141/73.
14. Direktiva Sveta 91/308/EGS. *Uradni list Evropskega Parlamenta š*t. 308/1991 – L 166.

15. *FATF – The Financial Action Task Force.* Najdeno 10. januarja 2016 na spletnem naslovu http://www.fatf-gafi.org
16. *FICO Tonbeller*. Najdeno 10. januarja 2016 na spletnem naslovu http://www.tonbeller.com/en/
17. Giraldo, J. K. (2007). *Terrorism financing and state responses: a comparative perspective.* Stanford: Stanford University Press.
18. Heracleous, L. (1994). *Rational Decision Making: Myth or Reality?* Najdeno 26. avgusta 2016 na spletnem naslovu https://www.researchgate.net/ publication/235302990_Rational_Decision_Making_Myth_or_Reality
19. *IMF Compliance with the AML/CFT international standards.* Najdeno 7. maja 2016 na spletnem naslovu https://www.imf.org/external/pubs/ft/wp/2011/wp11177.pdf
20. Iwanicz-Drozdowska, M. (2008). *Finance and real economy: selected research and policy issues*. Katowice: Karol Adamiecki University of Economics.
21. Jones, C. (2013). *Customer Due Diligence – Turning the tables on fraud.* Najdeno 27. avgusta 2016 na spletnem naslovu http://blogs.sas.com/content/sascom/2013/12/23/ customer-due-diligence-turning-the-tables-on-fraud/#more-13560
22. Kalb, B. (1982). Scandal at the Pop's bank. *Time.* Najdeno 20. februarja 2016 na spletnem naslovu http://www.time.com/time/magazine/article/ 0,9171,922953,00.html
23. Kazenski zakonik Slovenije. *Uradni list RS*, št. št. 55/08, št. 66/08-KZ-1, št. 39/09-KZ-1A, št. 91/11-KZ-1B, št. 50/2012- KZ-1-UPB2.
24. Konvencija Združenih narodov proti korupciji. (2005). Najdeno 2. aprila 2016 na spletnem naslovu https://www.unodc.org/documents/treaties/ UNCAC/Publications/ Convention/08-50026_E.pdf
25. Konvencija Združenih narodov proti mednarodnemu organiziranemu kriminalu. (2003). Najdeno 2. aprila 2016 na spletnem naslovu https://www.google.si/ ?gws_rd=cr,ssl&ei=HOF7V9jPLoKRsgH257rwAw#q=konvencija+zdru%C5%BEenih +narodov+proti+mednarodnemu+kriminalu
26. Koveos, P. (2007). *Critical issues for the 21st century global economy: economics, finance, management & entrepreneurship.* Athens: Athens Institute for Education and Research.
27. *KPMG.* Najdeno 2. aprila 2016 na spletnem naslovu https://home.kpmg.com/xx/ en/home.html
28. KPMG. (b.l.). Information technology – tool for addressing you AML risks. Najdeno 2. aprila 2016 na spletnem naslovu http://www.kpmg.com/NZ/en/services/Advisory /Risk-Compliance/Forensic/Anti-Money-Laundering/Documents/Presentation-2-IT-solution .pdf
29. Lamberger, I. (2001). *Gospodarski kriminal*. Ljubljana: Ministrstvo za notranje zadeve RS.
30. *Letno poročilo Urada za PPDFT.* Najdeno 8. februarja 2016 na spletnem naslovu http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/predstavitev/letno_porocilo _2008_tiskovno.pdf

31. Lewis, D. (2016). Speech on the importance of the FATF Global Network. Najdeno 20. aprila 2016 na spletnem naslovu http://www.fatf-gafi.org/publications/fatfgeneral/documents/MONEYVAL-speech-importance-of-FATF-Global-Network.html
32. Masciandaro, D. (2007). *Black finance: The economics of money laundering*. Cheltenham (UK), Northampton (MA): Elgar.
33. Massimo, F. (2013, 13. junij). Radical Reform Looms for Vatican Bank. *Corriere della Sera*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.corriere.it/english/13_giugno_13/vatican-bank_34a023ca-d420-11e 2-9edc-429eec6f64c6.shtml
34. Mediana. (b.l.). *Metode kvalitativnega raziskovanja.* Najdeno 27. avgusta 2016 na spletnem naslovu http://www.mediana.si/raziskovalne-metode/metode-kvalitativnega-raziskovanja/
35. Ministrstvo za finance. (2015). Poročilo o delu urada republike Slovenije za preprečevanje pranja denarja za leto 2014. Najdeno 2. januar 2016 na spletnem naslovu http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/deloUrada/letno_porocilo_2014.pdf
36. Money-laundering settlements. (2012, 12. december). V *The Economist.* Najdeno 14. decembra 2015 na spletnem naslovu http://www.economist.com/blogs/graphicdetail/2012/12/focus-1?zid=300&ah=e7b9370e170850b88ef129fa625b13c4
37. Muzenič, D. (2015). *Novosti Zakona o preprečevanju pranja denarja in financiranja terorizma. Posvet o odkrivanju in preprečevanju pranja denarja.* Ljubljana: Združenje bank Slovenije.
38. *Office of Foreign assets Control*. Najdeno 16. decembra 2015 na spletnem naslovu http://www.ustreas.gov/ofac
39. ORACLE. (2010). Best Practices for Anti Money Laundering (AML): System Selection and Implementation. Najdeno 2. aprila 2016 na spletnem naslovu http://www.oracle.com/us/industries/financial-services/062008.pdf
40. Organisation for Economic Co-operation and Development. (2009). Money Laundering Awareness handbook for Tax Examiners and Tax Auditors. Najdeno 20. decembra 2015 na spletnem naslovu http://www.oecd.org/tax/exchange-of-tax-information /43841099.pdf
41. Podzakonski predpisi in pravilniki ZPPDFT. *Uradni list RS* št. 10/08.
42. *Poročevalec državnega zbora RS, št. 32/XXXIII,* Ljubljana 2007, str. 4-6. Najdeno 28. marca 2016 na spletnem naslovu http://imss.dz-rs.si/imis /3eeedc9e76c81082f107.pdf
43. *Predlog osnutka Zakona o preprečevanju pranja denarja in financiranja terorizma*. Najdeno 14. decembra 2015 na spletnem naslovu http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Osnutek_predloga_ZPPDFT__JO.pdf
44. Protivity. Risk and Business Consulting. Internal Audit. (2013). Factors to consider When Selecting an AML Transaction Monitoring System. Najdeno 25. aprila 2016 na spletnem naslovu https://www.protiviti.com/en-US/Documents/POV/POV-AML-Transaction-Monitoring-System-Selection-Protiviti.pdf

45. PWC. (2010). From source to surveillance: the hidden risk in AML monitoring system optimization. Najdeno 3. aprila 2016 na spletnem naslovu http://www.pwc.com/us/en/anti-money-laundering/publications/assets/aml-monitoring-system-risks.pdf
46. PWC. (b.l.). *Anti-Money Laundering.* Najdeno 25. avgusta 2016 na spletnem naslovu http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html
47. *Referenčni model.* Najdeno 2. januarja 2010 na spletnem naslovu http://www.fu.unilj.si/iiu/Clanki/Uporabareferencnihmodelovpriprenoviposlovanja(37).pdf
48. Revizijski svet Slovenskega inštituta za revizijo (2007, november). Smernice za analizo tveganja vpletenosti stranke v pranje denarja in financiranje terorizma ter smernice za identifikacijo politično izpostavljenih oseb. Najdeno 20. januarja 2016 na spletnem naslovu www.si-revizija.si/revizorji/ dokumenti/smernice-analiza-ident.pdf
49. Schott, P. A. (2009). *Reference guide to antimoney laundering and combating the financing of terrorism* (2nd ed.). Washington: The World Bank – International monetary fund.
50. *Smernice za preprečevanje pranja denarja in financiranje terorizma za pravne in fizične osebe, ki opravljajo posle v zvezi z dejavnostjo računovodskih storitev*. (2010). Ljubljana: Urad za preprečevanje pranja denarja.
51. *Smernice za izvajanje zakona o preprečevanju pranja denarja in financiranja terorizma*. (b.l.). Najdeno 11. januarja 2016 na spletnem naslovu http://www.uppd.gov.si/si/zakonodaja_in_dokumenti/smernice/
52. Svet Banke Slovenije. (2008). *Usmeritve pri izvajanju ukrepov na področju PPDFT za bančni sektor*. Ljubljana: Banka Slovenije.
53. Šeme-Hočevar, V. (2006). *Globalizacija problema pranja denarja* (doktorska disertacija). Maribor: Univerza v Mariboru, Pravna fakulteta.
54. Šeme-Hočevar, V. (2006). Globalizacija problema pranja denarja. *Bančni vestnik*, 55, 14–17.
55. Šeme-Hočevar, V. (2007). *Pranje denarja: učinkovito odkrivanje in preprečevanje pranja*. Ljubljana: GV Založba.
56. *The fourth EU Anti Money laundering Directive*. Najdeno 3. januarja 2016 na spletnem naslovu https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf
57. Thony, J.F. (2000). *Money laundering and terrorism financing: An overview.* Najdeno 28. avgusta 2016 na spletnem naslovu https://www.imf.org/external np/leg/sem/2002/cdmfl/eng/thony.pdf
58. *Unicredit banka Slovenija, d.d.* Najdeno 20. januarja 2010 na spletnem naslovu http://www.unicreditbank.si/?language=SLO
59. United Nations office on Drug and Crime. (b.l.). *UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing*. Najdeno 13. decembra 2016 na spletnem naslovu https://www.unodc.org/unodc/en/money-laundering/Instruments-Standards. html?ref=menuside

60. United Nations Treaty Collection. (1988). *United Nations Convention against illicit traffic and narcotic drugs and psychotropic substances*. Najdeno 15. decembra 2015 na spletnem naslovu https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20VI/VI-19.en.pdf
61. *Urad za preprečevanje pranja denarja*. Najdeno 20. januarja 2010 na spletnem naslovu http://www.uppd.gov.si/
62. *Usmeritve pri izvajanju ukrepov na področju PPDFT za bančni sektor*. (2008). Najdeno 20. januarja 2010 na spletnem naslovu http://www.bsi.si
63. Veselko, V. (2004). *Preprečevanje pranja denarja: primer Slovenije* (diplomsko delo). Ljubljana: Ekonomska Fakulteta.
64. Witherell, W. (2002). International approaches to combating financial abuse and promoting stable financial markets. Najdeno 20. januarja 2010 na spletnem naslovu http://www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=70A8175028C6A96F553EBEA4D8AE1885?contentType=Article&contentId=1648514
65. Zakon o bančništvu (Zban-1). *Uradni list RS*, št. 99/2010 UPB-5, 52/11 – popr., 9/11 – ZPlaSS-B, 35/11, 59/11, 85/11, 48/12, 105/12, 56/13, 63/13 – ZS-K, 96/13, 25/15 – ZBan-2 in 27/16 – ZSJV.
66. Zakon o preprečevanju pranja denarja. *Uradni list RS*, št. 36/94, št. 63/95, št. 12/96 – ORZPPD28, št. 29/99, št. 79/01. Najdeno 20. januarja 2010 na spletnem naslovu http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4684
67. Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT). *Uradni list RS*, št. 60/07, 19/10, 77/11, 108/12 – ZIS-E in 19/14.
68. Zakon o spremembah in dopolnitvah Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-A). *Uradni list RS*, št. 19/10.
69. Zakon o spremembah in dopolnitvah Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-B). *Uradni list RS*, št. 77/11.
70. Zakon o spremembah in dopolnitvah Zakona o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-C). *Uradni list RS*, št. 19/14.
71. Žerjal, Ž. (2008). *Globalizacija preprečevanja pranja denarja in izzivi bančnega sektorja* (magistrsko delo). Ljubljana: Ekonomska fakulteta.

PRILOGE

KAZALO PRILOG

Priloga 1: Seznam kratic

- CFSP – Skupna zunanja varnostna politika (angl. *Common foreign security policy*)
- FATF – Projektna skupina za finančno ukrepanje (angl. *Financial action task force on money laundering*)
- FATCA - Zakon o spoštovanju davčnih predpisov v zvezi z računi v tujini (angl. *Foreign Account Tax Compliance Act*)
- FIU – Enota za finančni nadzor (angl. *Financial intelligence unit*)
- GPML – Globalni program proti pranju denarja (angl. *Global antimoney laundering programme*)
- IMF – Mednarodni denarni sklad (angl. *International monetary fund*)
- ISIL – Islamska država (angl. *Islamic State of Iraq and the Levant*)
- IT – Informacijska tehnologija (*Information Technology*)
- KZ – Kazenski zakonik
- KYC - Poznavanje stranke (angl. *Know your customer*)
- OECD – Organizacija za gospodarsko sodelovanje in razvoj (angl. *Organization for economic cooperation and development*)
- OFAC – Urad za nadzor tujih sredstev (angl. *Office of foreign assets control*)
- PEP – Politično izpostavljena oseba (angl. *Politically Exposed Person*)
- PPD – Preprečevanje pranja denarja
- PPDFT – Preprečevanje pranja denarja in financiranja terorizma
- UNODC - Urada Združenih narodov za droge in kriminal (angl. *United Nations office on Drugs and Crime)*
- ZN – Združeni narodi
- ZPPDFT – Zakon o preprečevanju pranja denarja in financiranja terorizma