Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KORIŠTENJE ELEKTRONSKOG I KORESPONDENTNOG BANKARSTVA ZA AKTIVNOSTI PRANJA NOVCA

USE OF ELECTRONIC AND CORRESPONDENT BANKING FOR MONEY LAUNDERING ACTIVITIES

Stručni rad

Ajla Šurković, MA[465]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljavaju: Napredak u razvoju informacione tehnologije uticao je na pojavu novih oblika pranja novca koje karakteriše sofisticiranost, prikrivenost, veći nivo organizacije, međunarodni karakter kao i kreativnost kriminalaca. Elektronski transferi novca sa jednog računa na drugi, te brzina kojom se isti realizuje omogućava prikrivanje stvarnog izvora tog novca.

Ciljevi rada (naučni i/ili društveni): Naučni cilj rada ogleda u opisivanju faktora koji utiču na pojavu pranja novca u elektronskom i korespondentnom bankarstvu. Društveni cilj odnosi se na informisanje akademske i stručne javnosti o specifičnostima pranja novca korištenjem elektronskog i korespondentnog bankarstva.

Metodologija/Dizajn: Pri izradi rada koristit će se literatura domaćih i stranih autora te ostali naučni i stručni članci dostupni na internetskim stranicama. U radu će biti korištene sljedeće metode: metoda analize te deduktivna i induktivna metoda. Kada je u pitanju metoda prikupljanja podataka bit će korištena analiza sadržaja.

Ograničenja istraživanja/rada: Ograničenje ovog rada je teorijsko razmatranje pranja novca korištenjem elektronskog i korespondentnog bankarstva. Naime, u istom će biti prikazana postojeća naučna saznanja kada je u pitanju predmet istraživanja. Stoga, ovim radom nije moguće ukazati na praktična rješenja koja bi mogla uticati na sprečavanje pranja novca u oblastima koje će biti obrađene u radu.

Rezultati/Nalazi: Pranje novca korištenjem elektronskog bankarstva iako obuhvata tri tradicionalne faze pranja novca ima određene specifičnosti u pogledu mjesta i načina na koji se preduzimaju određene aktivnosti. Internet bankarstvo i Mobilno bankarstvo kao distrubucijski kanali elektronskog bankarstva mogu omogučiti prikrivanje kako porijekla novčanih sredstava tako i identiteta klijenata koji koriste te usluge što povećava rizik od pranja novca. S druge strane, korespondentno bankarstvo se koristi za aktivnosti pranja novca jer predstavlja vrstu poslovnog odnosa koji omogućava poslovanje sa rezidentnom bankom bez tačnih i pouzdanih informacija o porijeklu novčanih sredstava. Posebno su rizični korespondentni odnosi sa *shell* bankama koje fizički ne postoje niti u jednoj zemlji te osnivanje ofšor finansijskih centara pomoću kojih određene pravne i fizičke osobe ostvaruju „finansijske pogodnosti“.

[465] ajlasurkovic@fkn.unsa.ba

Generalni zaključak: Uzimajući u obzir zajedničku karakteristiku elektronskog i korespondentnog bankarstva koja se odnosi na fizičko odsustvo stranaka sa kojima se vrši poslovanje, može se zaključiti da navedene djelatnosti pospješuju aktivnosti pranja novca.
Opravdanost istraživanja /rada: Opravdanost ovog rada ogleda se u spoznaji pojavnih oblika pranja novca koje su omogućili elektronski transferi.

Ključne riječi
pranje novca, elektronsko bankarstvo, korespondentno bankarstvo, *shell* banke

Abstract
Inspiration for the research and problem (s) referred to in this work: Progress in development of informational technologies has affected the emergence of new forms of money laundering that is characterized by sophistication, concealment, higher level of organisation, international character as well as the creativity of criminals. Electronic transfers of money from one back account to another and the speed of its realization, allows a cover-up of the true money source.
Research goals (scientific and/or social): Scientific goal reflects itself in the description of factors that affect the emergence of money laundering within electronic and correspondent banking. Social goal refers to the informing of academic and expert public regarding specifics of money laundering using electronic and correspondent banking.
Methodology/Design: During the execution of this work, literature of regional and foreign authors will be used as well as other scientific articles and articles of expertise available on internet sites. In said work following methods will be used: method of analysis, and deductive and inductive method. Regarding the data collecting method, content analysis will be used.
Limitations in the research/work: The limitation of this particular work lies in the theoretical deliberation of money laundering through electronic and corresponding banking. More specifically, through said deliberation, existing scientific findings in reference to the subject of research will be presented. Therefore in this work, it is not possible to address practical solutions that would affect prevention of money laundering within areas included in this research.
Results/Findings: Although it includes three traditional phases, money laundering through the use of electronic and correspondent banking has certain specifics in regards to the place and the way certain activities are done. Internet Banking and Mobile Banking as channels for electronic banking distribution can allow for concealment of origin of funds as well as the identity of clients, increasing the risk of money laundering. On the other hand, correspondent banking is being used for money laundering activities because it presents a form of business relationship that allows for commerce with the residential bank without precise and reliable information about the origin of the funds. Especially risky are correspondent relations with "shell" banks that physically do not exist in any country, as well as establishment of "off-shore" centers that provides certain legal and physical persons with certain "financial benefits".
General Conclusion: Considering a common characteristic of electronic and correspondent banking related to the physical absence of parties with which business relationship is established, it can be concluded that said activities enhance money laundering activities.
Validity of the research/work: This work's validity reflects itself within the acknowledgement of manifestations of money laundering enabled by electronic transfers.

Keywords
money laundering, electronic banking, correspondent banking, *shell* banks

Uvod

Pranje novca predstavlja aktivnost usmjerenu na prikrivanje stvarnog porijekla novčanih sredstava te ulaganja isti u finansijski i nefinansijski sistem s ciljem njegove legalizacije. S obzirom na njegovu učestalost, pranje novca je opisano kao kriminal 90-tih, pa čak i kao kriminal 21. stoljeća (Madinger, 2012, str. 300). Napredak u razvoju informacione tehnologije uticao je na pojavu novih oblika pranja novca koje karakteriše sofisticiranost, prikrivenost, veći nivo organizacije, međunarodni karakter kao i kreativnost kriminalaca. Pojava novih finansijskih usluga (mobilno bankarstvo, internet bankarstvo) i sistema plaćanja (elektronsko plaćanje) stvara uslove koji povećavaju rizik od pranja novca. Elektronski transfer novca sa jednog računa na drugi, te brzina kojom se isti realizuje omogućava prikrivanje stvarnog izvora novca.

U ovom radu bit će predstavljeno korištenje elektronskog i korespondentnog bankarstvo za aktivnosti pranja novca. „Prema Odluci o upravljanju informacionim sistemom u banci, Agencije za bankarstvo Federacije Bosne i Hercegovine, član 2. pod n) elektronsko bankarstvo je sistem koji omogućava klijentima banke obavljanje bankarskih poslova sa udaljene lokacije putem javnih komunikacionih mreža ili slično.“ Korespondentsko bankarstvo je pružanje bankarskih usluga jedne banke drugoj banci, što podrazumijeva postojanje korespondentskog računa jedne finansijske institucije koji ona drži kod druge finansijske institucije za svoj račun i u svoje ime (Zirojević, 2017. str. 19).

Naučni cilj rada ogleda u opisivanju faktora koji utiču na pojavu pranja novca u elektronskom i korespondentnom bankarstvu. Društveni cilj odnosi se na informisanje akademske i stručne javnosti o specifičnostima pranja novca korištenjem elektronskog i korespondentnog bankarstva. Kada je u pitanju struktura rada, prvi dio se odnosi se na definisanje pranje novca, faze od kojih se sastoji, krivično pravno određenje kao i karakteristike istog. U drugom dijelu rada, prije svega, je definisano elektronsko bankarstvo, zatim, prikazani domaći i međunarodni napori usmjereni na sprečavanje zloupotrebe istog i na kraju, predstavljeni mobilno i internet bankarstvo kao distributivni kanali elektronskog bankarstva. Korespondentno bankarstvo, kao specifičan oblik poslovnog odnosa i mogućnosti njegovog korištenja za aktivnosti pranja novca prikazani su u trećem dijelu rada.

Pri izradi rada koristit će se literatura domaćih i stranih autora te ostali naučni i stručni članci dostupni na internetskim stranicama. U radu će biti korištene sljedeće metode: metoda analize te deduktivna i induktivna metoda. Kada je u pitanju metoda prikupljanja podataka bit će korištena analiza sadržaja. Ograničenje ovog rada je teorijsko razmatranje pranja novca korištenjem elektronskog i korespondentnog bankarstva.

Naime, u istom će biti prikazana postojeća naučna saznanja kada je u pitanju predmet istraživanja. Stoga, ovim radom nije moguće ukazati na praktična rješenja koja bi mogla uticati na sprečavanje pranja novca u oblastima koje će biti obrađene u radu.

Pranje novca

Pranje novca predstavlja fenomen kojim osobe koje su stekle novac na nezakonit način nastoje prikriti stvarno porijeklo istog. Pojam "pranje novca" odnosi se na sve vrste postkriminalnih aktivnosti usmjerenih na prikrivanje imovinske koristi ili vrijednosti stečene na nezakoniti način (Meštrović, 2002). U ekonomskom smislu sam pojam pranja novca znači legalizacija kapitala stečenog kriminalnom djelatnošću, odnosno finansijske transakcije radi prikrivanja stvarnog porijekla novca i drugih oblika kapitala na tržištu (Bjelopoljak, 2012). Kako bi postigli navedeno osobe koje se bave pranjem novca poduzimaju različite radnje te stalno usavršavaju svoje aktivnosti korištenjem različitih tehnika pranja novca. Zajedničke karakteristike tih tehnika su (Gilmor, 2006, str. 33):

- oni koji „peru" novac moraju da sakriju pravi identitet vlasnika i porijeklo novca,
- moraju da zadrže kontrolu nad sredstvima, i
- moraju da promjene oblik sredstava.

Sofisticiranost, inventivnost i maštovitost raznih oblika pranja novca obuhvaćaju i usluge raznih financijskih stručnjaka, poreznih savjetnika, brokera, investicijskih kuća, konzultanata i advokata (Cindori, 2010, str. 20).

Pranje novca kao krivično djelo propisano je članom 209. Krivičnog zakona Bosne i Hercegovine te je stavom 1. istog definisan je osnovi oblik krivičnog djela pranja novca određeno je sljedeće:

1. „Ko novac ili drugu imovinu za koje zna da su pribavljeni počinjenjem krivičnog djela primi, zamijeni, drži, raspolaže njima, koristi u privrednom ili drugom poslovanju, vrši konverziju ili njihov prijenos ili na drugi način prikrije ili pokuša prikriti njihovu prirodu, izvor, lokaciju, raspolaganje, kretanje, vlasništvo ili drugo pravo, a takav novac ili imovinska korist su pribavljeni počinjenjem krivičnog djela:

a. u inostranstvu ili na teritoriji cijele Bosne i Hercegovine ili na teritoriji dvaju entiteta ili na teritoriji jednog entiteta i Brčko Distrikta Bosne i Hercegovine; ili
b. koje je propisano Krivičnim zakonom Bosne i Hercegovine ili drugim zakonom na državnom nivou, kaznit će se kaznom zatvora u trajanju od jedne do osam godina.

Članom 2. u stavovima a) i b) Zakona o sprečavanju pranja novca i finansiranja terorističkih aktivnosti određeno je sljedeće:

a) „Pranje novca podrazumijeva:

1. zamjenu ili prijenos imovine, ako je ta imovina stečena kriminalnim radnjama, a s ciljem prikrivanja ili zataškavanja nezakonitog porijekla imovine ili pružanja pomoći nekom licu koje je umiješano u takve aktivnosti radi izbjegavanja zakonskih posljedica počinjenih radnji;
2. prikrivanje ili zataškavanje prave prirode, mjesta porijekla, raspolaganja, kretanja, prava na ili vlasništva nad imovinom ako je ta imovina stečena kriminalnim radnjama ili činom učešća u takvim radnjama;
3. sticanje, posjedovanje ili korištenje imovine stečene kriminalnim radnjama ili činom učešća u takvim radnjama;
4. učešće ili udruživanje radi izvršenja, pokušaja izvršenja, odnosno pomaganja, podsticanja, olakšavanja ili davanja savjeta pri izvršenju bilo koje od navedenih radnji;
5. svrha, znanje, namjera potrebni kao elementi radnje pranja novca mogu se zaključiti na osnovu objektivnih i činjeničnih okolnosti.
6. pranjem novca smatrat će se i to kada su radnje, kojima je stečena imovina koja se pere, izvršene na teritoriji druge države."

Suština pranja novca je transformacija potencijalne kupovne moći[466] u djelotvornu (Madsen, 2009). Navedeno se postiže pretvaranjem „prljavog" novca u bankovni saldo, te uklanjanje njegove očigledne veze sa kriminalnim aktivnostima (Siwi, (2018). Dakle, cilj je promjena nezakonito stečenih novčanih sredstava u neki drugi oblik imovine nastojeći prikriti njegov nezakonit izvor. Iako proces pranja novca izgleda veoma komplikovano, isti uglavnom obuhvata tri faze i to: plasiranje, uslojavanje i integraciju[467] (Bjelopoljak, 2012). Različite finansijske usluge i platni sistemi omogućava bezbroj mogućnosti za stvaranje komplikovanih shema za prijenos novca. Pojava Interneta uticala je na nastajanje novih pojavnih oblika pranja novca kojim osobe koje se bave tim aktivnostima nastoje prikriti nezakonito stečen prihod. Novi pojavni oblici pranja novca povezani su s elektronskim poslovanjem i transakcijama realiziraju se putem korespondentnih računa, kreditnih kartica, Internet bankarstva, smart kartica i sl. U svrhu dugotrajnog pranja novca, može se koristiti novac uložen u firme, turističke objekte ili kockarnice. U slučajevima kada se pranje novca vrši uz pomoć gotovine, novac će se najčešće vraćati putem korespondentnog bankarstva u zemlju porijekla, u skladu s međunarodnim platnim prometom (Savić, 2016, str. 12).

[466] „Polman, Effron i Thomas (2018) kupovna moć ima osnovno svojstvo novca. Novac ima vrijednosti jer se može zamijeniti za robu ili uslugu, a stepen njegove vrijednosti zavisi od količine i kvaliteta robe ili usluge koja se može kupiti."

[467] Vidjeti više u: Savona, U. E. (1997). *Responding to money laundering: international perspectives.* Harwood Academic Publishers; 1 edition, str.23-27.

Elektronsko bankarstvo

Stalne tehnološke inovacije utiču na razvoj bankarskih proizvoda i usluga koje su stanovništvu dostupne putem elektronskih distributivnih kanala. Novi bankarski proizvodi i usluge uključuju elektronsko bankarstvo koje predstavlja upotrebu bankarskih usluga i izvođenje bankarskih transakcija koje obavlja sama stranka, vlasnik računa i komitent banke, posredstvom osobnih računara ili terminala s lokacija s kojih je moguć pristup telekomunikacijskoj mreži za prijenos podataka (Leko, 1998). Dostupnost različitih, prilagodljivih i cjenovno konkurentnih bankovnih usluga uz upotrebu modernih tehnologija, postaje temelj današnjeg bankarstva i društva (Bejatović i Kovačević, 2009).

Elektronsko bankarstvo predstavlja poslovanje kreditnih institucija pomoću telekomunikacijske mreže, a uključuje sve proizvode i usluge dostupne strankama tim putem te poslove koje kreditna institucija obavlja u svoje ime i za svoj račun koristeći se navedenim distribucijskim kanalom (Porobić, Bajraktarević, 2012, str. 85). Elektronskim se transferima teško ulazi u trag upravo zbog minimuma identifikacijskih informacija o stranci, čime se omogućava međunarodno kretanje ogromnih iznosa novca u samo jednoj sekundi. „Samo se jedan takav transfer kreće u rasponu i do milion dolara, dok procjene govore da se na dnevnoj razini razmjenjuju čak i trilioni dolara (u novčanicama i obveznicama (Savona, 2004, str. 153-154).

Kao i tradicionalni oblici pranja novca, pranje novca korištenjem elektronskog bankarstva obuhvata fazu plasmana, uslojavanja i integraciju. „Prema Daniali (2014) u fazi plasmana osobe koje koristeći usluge elektronskog bankarstva kupuju proizvode čiju vrijednost je teže utvrditi te je navedena aktivnost manje rizična. U fazi uslojavanja anonimnost i brzina koje karakterišu elektronsko bankarstvo onemogućava „ulazak u trag“ sumnjivim aktivnostima. Pranje novca u fazi integracije odvija se putem različitih metoda poput ulaganja, krivotvorenja isprava, transakcija prodaje i kupnje čije otkrivanje je teže jer se iste obavljaju u virtualnom prostoru.“

S ciljem sprečavanja pranja novca donesen je Zakon o sprečavanju pranja novca i finansiranju terorističkih aktivnosti. Istim je u članu 32. određeno da „pružalac usluge plaćanja i naplate dužan je prikupiti tačne i potpune podatke o nalogodavcu i uključiti ih u obrazac ili poruku koja prati elektronski transfer sredstava poslatih ili primljenih, bez obzira na valutu. Ti podaci moraju pratiti elektronski transfer tokom cijelog puta u lancu plaćanja, bez obzira na to da li posrednici u lancu plaćanja postoje i bez obzira na njihov broj.“

Međunarodni napori sprečavanja pranja novca i finansiranja terorizma putem elektroniskih transfera novca, a samim time i elektronskog bankarstva, istaknuti su u tački 14.

uvoda Treće direktive[468], članu 26. Zakona o sprečavanju pranja novca i finansiranja terorizma[469], kao i u VII Specijalnoj preporuci FATF koja ističe značaj i opasnosti napredne tehnologije.

Nivoi elektronskog bankarstva su različiti. U nastavku će biti taksativno prikazani (Yubin, 2003):

1. Osnovne e-bankarske informacije – web sajtovi koji informišu o bankarskim proizvodima i uslugama;
2. Jednostavne e-bankarske transakcije – web sajtovi koji nude upotrebu aplikacija za postavljanje upita o računima klijenta, ali bez mogućnosti transfera novca;
3. Napredne e-bankarske transakcije – web sajtovi koji klijentima omogućuju elektronski transfer na/sa računa, kao i onlajn upravljanje drugim bankarskim transakcijama.

Prednosti banaka koje koriste elektronsko bankarstvo su brojne. Neke od njih su (Vuksanović, 2006, str. 218):

- Stvaranje imidža inovativne firme koja je u stanju da svojim korisnicima ponudi najsavremenija tehnološka rješenja;
- Veće i bolje interaktivne mogućnosti – za banku koja se u tržišnim uslovima bori za svakog svog komitenta, najvažnija je komunikacija sa njim;
- Mogućnost racionalizacije potencijala banke – banka prenošenjem određenih servisa na internet smanjuje troškove poslovanja jer ne mora zbog povećanja broja komitenata da otvara novi poslovni prostor, da ga oprema i zapošljava nove službenike. Ovo je posebno interesantno za one geografske regione gdje banka nema mrežu ekspozitura ili ima mali broj komitenata;
- Samouslužno bankarstvo je korisno podjednako i za banku i za komitenta, jer komitent ima servise 24 časa dnevno, 7 dana u nedelji, a banka bez povećanja broja zaposlenih tako radi 365 dana u godini;
- Banka svojom pojavom na internetu dokazuje svoje konkurentne mogućnosti i svoj razvoj kao solidna, stabilna i tehnološki napredna firma

Primjena informacione tehnologije u bankarstvu praćena ekspanzijom elektronskog novca i elektronskog bankarstva nosi sa sobom pojavu novih oblika rizika. Pritom je

[468] Tačka 14. uvoda Treće direktive njezin obuhvat proširuje na sve radnje radnje koje institucije i osobe obuhvaćene direktivom obavljaju na Internetu.
[469] Članom 26. Zakona o sprečavanju pranja novca je propisana obaveza kreditnim i finansijskim institucijama, uključujući društva koja obavljaju određene usluge platnog prometa ili prijenosa novca prikupljanja tačnih i potpunih podataka o uplatiocu i uključiti ih u obrazac ili poruku koja prati elektronski prijenos novčanih srestava, poslanih ili primljenih u bilo kojoj valuti.

potrebno posebnu pažnju obratiti na upravljanje rizikom[470] koji proizlazi iz korištenja informacijskog sistema kako bi poslovanje banke bilo sigurno. Iako je osiguranje sigurnosti suštinski problem, set specifičnih rizika čine: operativni rizik[471], reputacioni rizik, pravni rizik, rizik internacionalnog poslovanja i ostali rizici.

Korištenje distributivnih mreža elektronskog bankarstva za aktivnosti pranja novca

Dio distributivne mreže elektronskog bankarstva čine Internet bankarstvo i Mobilno bankarstvo. Kako navodi Antonić (2012) Internet bankarstvo predstavlja obavljanje bankarskog poslovanja direktno od kuće, putem Interneta. Banka pruža usluge i omogućava plaćanje roba i usluga preko Interneta, izdaje platne kartice, otvara tekuće račune, obavlja mjenjačke poslove, omogućava provjeru stanja na računu vrši transfer elektronske gotovine i drugo. Internet bankarstvo je jedan od najpoznatijih načina za pranje novca u takozvanom sajber okruženju. Naime, zloupotrebom Internet bankarstva u svrhe pranja novca, banka može posredstvom svog servera da potvrdi da je klijent pristupio serveru sa određenog računa, u određeno vrijeme i veličinu transakcije koja je obavljena, ali nema mogućnost da izvrši tačnu identifikaciju klijenta, niti sa kojeg mjesta je pristupljeno serveru što omogućava da jedno lice kontroliše veliki broj računa i izvršava veliki broj transakcija bez znanja banke (Antonić, 2012, str. 68-69). Pored toga, osobe koje se bave aktivnostima pranja novca nastoje prenijeti nezakonito stečen novac putem regularnih finansijskih posrednika takozvanih „novac mazgi[472]“. „Novac mazge“ su veoma korisne kriminalnih organizacijama, jer se na taj način onemogućava otkrivanje glavnih aktera. Bankovni računi su otvoreni na ime „novac mazge“ koje se iskorištavaju od strane organiziranih kriminalnih grupa. Nekoliko studija potvrđuje važnu ulogu „novac mazgi“ u preusmjeravanju novca ukradenog od strane sajber (cyber) kriminala koji se bave

[470] „Kako navode (Poborić, Bajraktarević, 2012, str. 89) „na osnovu obavljene procjene rizika banka će, izmjenu ostalog, odrediti adekvatne kriptografske metode čija će primjena smanjiti rizik od narušavanja temeljnih načela informacijskog sistema. Kriptografske metode predstavljaju jednu vrstu logičkih kontrola kojima se dodatno osigurava zaštita informacija i smanjuje rizik od narušavanja temeljnih načela informacijskog stava. Kriptografija se najčešće upotrebljava za enkripciju (šifriranje podataka), elektronsko potpisivanje, očuvanje integriteta podataka i utvrđivanje autentičnosti korisnika (verifikacija stranke)“.

[471] Baselski odbor za nadzor banaka (2011) definirao je operativni rizik kao „rizik od gubitaka koji nastaje zbog neprimjerenih ili neuspješnih unutarnjih procesa, ljudi ili sistema ili zbog vanjskih događaja“.

[472] „Novac mazge“ je termin koji podrazumijeva osobe koje kriminalci iskorištavaju s ciljem prijenosa novca sa bankovnih računa. Te osobe se obično regrutuju putem oglasa uvjeravajući ih da će na taj način mogu zaraditi dosta novca (Bank safe online, 2008).

finansijskim krivičnim djelima u sajber okruženju, kao što su karding (carding)[473] i fišing (pfishing)[474] napadi.

Osim korištenja „novac mazgi" s ciljem izbjegavanja krivičnog progona novac se djeli na manje iznose koji ne zahtijevaju izvještavanje nadležnih organa od strane finansijskih institucija, te se na taj način može brzo i lahko izvršiti prijenos sa jednog na više bankovnih računa u više finansijskih institucija (Weaver, 2005). Kao što je istaknuto u izvještaju Vijeća Evrope, na osnovu studija slučaja otkriveno je da su osobe koje se bave aktivnostima pranja novca ponekad provodili stotine besmislenih transakcija preko različitih bankovnih računa, nakon čega slijedi ograničen broj podizanja gotovine (Council of Europe, 2012).

Mobilno bankarstvo kao dio distributivne mreže elektronskog bankarstva obuhvata finansijske transakcije preduzete korištenjem mobilnog uređaja. Mobilno bankarstvo je fenomen koji se nedavno pojavio, posebno u zemljama u razvoju, potaknut rastućom potražnjom za mikro-plaćanjem (Fiedler, 2013). Mobilna plaćanja obavljaju se korištenjem različitih protokola te telekomunikacijski operateri djeluju kao finansijski posrednici između klijenta i poslovnih subjekata, odnosno klijenta i finansijske institucije (Filipkowski, 2008). Mogućnost kupovine SIM kartice bez provjere identiteta omogućava anonimnost osobe koja vrši mobilno plaćanje što koriste „perači" novca (Villasenor, Bronk i Monk, 2011). Pitanja o kojima se često raspravlja kada je riječ o mobilnom bankarstvu odnose se na pitanje autentičnosti, poznavanja klijenata, autorizacije i integriteta transakcije, praćenja iznosa koje pojedinci imaju na raspolaganju kao i onih koje šalju (Bamoriya, 2016).

Korespodentno bankarstvo

Članom 3. Zakona o sprečavanju pranja novca i finansiranju terorističkih aktivnosti pod k) propisano je "korespondentni odnos je odnos između domaće banke ili druge finansijske institucije i strane banke ili druge finansijske institucije koji nastaje otvaranjem računa strane banke ili druge finansijske institucije kod domaće banke ili druge finansijske institucije ili uspostavljanjem bilo kojeg drugog poslovnog odnosa, kao i kada domaća banka ili druga finansijska institucija otvara račun kod strane banke ili druge finansijske institucije ili uspostavlja bilo koji drugi poslovni odnos." Osnovna ideja korespondentnog bankarstva proizlazi iz nedostatka unutrašnje umreženosti respondentne banke, a obuhvaća: međubankarske depozitne aktivnosti, međunarodne elektronske transfere

[473] Karding (carding) predstavlja kombinaciju visokotehnološkog i sajber kriminala i uključuje skup tehnika pomoću kojih kriminalci prikupljaju informacije o kreditnim karticama i drugim informacijama vezanih za plaćanje te način korištenja tih informacija od strane istih (Meijerink, 2013).
[474] Fišing (phishing) je vrsta socijalnog inžinjeringa koji omogućava dobijanje ličnih podataka od strane korisnika računara (Ollman, 2004).

sistema, upravljanje gotovinom, cheque clearing[475] i usluge uplate, naplatu, procesuiranje uplata strankama (u domaćoj i stranoj valuti) te transfere putem payable-through accounts (Esoimeme, 2015, str. 93).

Poslovanje putem korespondentnog bankarstva podrazumijeva poslovnu saradnju prilikom koje banka primatelj nije obavezna raspolagati tačnim ili potpunim podacima o porijeklu novčanih sredstava koja su predmet uplate. (Weisman, 2014, str. 6). Vrsta poslovanja kojom posluje respondent, kao i tržište na kojem prodaje svoje usluge, korespondentu ukazuju na visinu rizika koji mu respondent predstavlja (Cindori i Petrović, 2016, str. 769).

Problem predstavljaju korespondentni odnosi s visoko rizičnim bankama koje imaju manjkavu pravnu regulativu, nepouzdani (ili korumpirani) menadžment, a samim time i lošu preventivnu strategiju suzbijanja pranja novca i finansiranja terorizma. U visoko rizične strane banke mogu se ubrojiti (Porobić, Bajraktarević, 2012, str. 92):

- *shell* banke – koje fizički ne postoje niti u jednoj zemlji;
- *offshore* banke – kojima je licenca ograničena na poslovanje samo s osobama izvan teritorija te zemlje ili joj je onemogućeno poslovanje s lokalnom valutom;
- banke koje se nalaze unutar države koja ne primjenjuje odgovarajuće standarde ili ne sarađuje u međunarodnim nastojanjima sprečavanja pranja novca i finansiranja terorizma.

Shell banke (fiktivne banke) se članom 3. stav 1. tačka 10. Treće direktive definiraju kao kreditne institucije ili institucije za obavljanje istovjetnih poslova, inkorporirane u nadležnost države u kojoj nisu fizički prisutne (uključujući autentičnost i menadžment), a nisu povezane niti sa zakonski regulisanom finansijskom grupom. U skladu sa principima Wolfsberg grupe, banke imaju obavezu odbiti uspostavu ili nastavak korespondentnog bankarstva s bankom koja je osnovana u jurisdikciji u kojoj nije fizički prisutna i povezana s normativno uređenom finansijskom grupom, poput *shell* banke (Esoimeme, 2015, str. 93).

Termin ofšor (engl. offshore) je iz engleskog prava, odnosno *common law* pravnog sistema, a prevodi se kao eksteritorijalno područje. Ovaj oblik poslovanja obavljao se na ostrvima izvan teritorije Velike Britanije, te je tako i nastao sam termin, a važio je za sva područja koja finansijskim institucijama nude specijalne pogodnosti, te se iste ogledaju u liberalnim ekonomskim i poreskim propisima. „Kako navode (Čudan i Fijat, 2015, str. 62)

[475] S obzirom na to da su međunarodni elektronski transferi pod povećanim nadzorom, „perači" novca mijenjaju oblik novca koristeći gotovinske čekove kao djelotvornu alternativu. Cheque clearing je transferiranje čeka iz banke u kojoj je položen do banke kod koje je podignut, dok se kretanje novca odvija u suprotnom smjeru (Weisman, 2014., str. 5–6).

ofšor centri su se počeli osnivati za vrijeme velike ekonomske krize 30-ih godina prošlog vijeka i to uz pomoć američkog organiziranog kriminala."

Razlog koji se najčešće navodi za osnivanje ofšor finansijskih centara jeste pružanje određenih „finansijskih pogodnosti" pravnim i fizičkim licima koja koriste njihove usluge, a te pogodnosti se najčešće koriste za legalizaciju ili skrivanje nelegalno stečenih sredstava (Bošković, 2005, str. 48). „Kako navodi Banović (2002) ovi finansijski centri imaju nekoliko osnovnih karakteristika:

- višestruki niz finansijskih transakcija,
- korištenje posrednika za njihovo izvođenje,
- razvijenost međunarodne mreže, takozvanih *shell* kompanija, uključujući i specijalizovane *off-the-shell* varijacije koje se gase odmah po završetku transakcije, kao i
- korištenje više ofšor centara za jednu operaciju pranja novca."

Prema Zirojeviću (2017) priroda korištenja korespondentskih računa stvara indirektan odnos u kojem korespondentska banka pruža bankarske usluge pravnim i fizičkim licima za koja ne postoje informacije o potvrdi identiteta. Pri tome se korespondentska banka oslanja na informacije respondentske banke. Uspostavljeni odnos se usložnjava u sljedećim slučajevima (Bošković, 2005, str. 39-40):

- kada se kao respondentska banka javlja ofšor finansijska institucija,
- kada je nemoguće procjeniti kvalitete mehanizama sprečavanja pranja novca iako postoji legislativa koja važi u respondentskoj banci,
- kada nije moguće nadgledati pojedinačne transakcije koje su uključene u velike transakcije između korespondentskih računa zato što banka nije u vezi sa pošiljaocem ili korisnikom tih transakcija i
- u slučajevima kada postoje podrespondenti, kada respondentska banka nudi korespondentske usluge.

Zaključak

Pranje novca predstavlja djelatnost koja obuhvata poduzimanje različitih aktivnosti s ciljem prije svega, prikrivanja nezakonito stečenih novčanih sredstava, a potom integraciju istih u legalne finansijske tokove. Dakle, pranje novca je proces koji se sastoji od tri faze, od plasmana „prljavog" novca do integracije istog. Radi postizanja navedenog koriste se različite tehnike od strane osoba koje se bave aktivnostima pranja novca. Pranje novca u sajber okruženju se vrši stvaranjem komplikovanih shema za prijenos novčanih sredstava koje je teško otkriti. Pojava elektronsko i korespondentno bankarstvo uticala je na razvoj novih pojavnih oblika pranja novca.

Elektronsko bankarstvo je dostupno stanovništvu putem elektronskih distributivnih kanala što omogućava obavljanje transakcija brzo i jednostavno. Takva vrsta poslovanja ima niz benefita kako za klijente koji na taj način mogu obavljati transakcije od kuće, tako i za banke koji pružanjem novih usluga postaju konkurenti na tržištu. Međutim, elektronsko bankarstvo može biti korišteno za aktivnosti pranja novca na različite načine, što zahtijeva procjenu rizika od strane finansijskih institucija te upravljanje istim.

Pranje novca korištenjem elektronskog bankarstva se ostvaruje na osnovu takozvanih „novac mazgi" koje predstavljaju osobe čije bankovne račune kriminalci upotrebljavaju s ciljem prijenosa novca koji je stečen na nezakonit način. Bankovni računi izloženi su sajber napadima s ciljem dobijanja ličnih podataka. Obavljaju više transakcija manjeg iznosa sa različitih računa na više različitih računa što otežava otkrivanje tih nezakonitih aktivnosti. Pored toga, mogućnost kupovine SIM kartice bez provjere identiteta kupca može uticati na korištenje mobilnog bankarstva radi pranja novca.

Korespondentno bankarstvo predstavlja oblast poslovanja koja omogućava pružanje usluga prijenosa novca sa računa jedne na račun druge banke uz određenu naknadu. Isto je izloženu riziku od pranja novca jer omogućava poslovanje sa rezidentnom bankom bez tačnih i pouzdanih informacija o porijeklu novčanih sredstava. Posebno su rizični korespondentni odnosi sa *shell* bankama koje fizički ne postoje niti u jednoj zemlji te bankama čije poslovanje je ograničeno samo na osobe u drugim zemljama. Stvaranjem tih ofšor centara je omogućeno skrivanje nezakonitih novčanih sredstava. U slučaju kada se kao rezidentna banka javlja ofšor finansijska institucija dolazi do usložnjavanja odnosa koji je uspostavljen u okviru korespodetnog poslovanja.

Literatura

1. Antonić, J. (2012). Abuse of Modern Technology of Money Laundering. *Economic outlook/Ekonomski pogledi,* 3, 66-79.
2. Bank safe online. (2008). Payment advice. Helpful information from the UK payments association.banke Money Mules. http://www.banksafeonline.org.uk/documents/money_mules_advice_guide_final.pdf pristupljeno 26.06.2019. godine.
3. Banović, B., (2002). *Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta*, Beograd,Viša škola unutrašnjih poslova.
4. Baselski odbor za nadzor banaka, (2011.), *Dobre prakse za upravljanje operativnim rizikom i nadzor nad njim*, Banka za međunarodne namire.
5. Bamoriya, P. (2016). Issues in Mobile Banking in India with references to Regulations. *Journal of Accounting & Management,* 6 (1), 17-34.
6. Bejatović, M i Kovačević, M. (2009), Elektronsko bankarstvo- EFT, *Pravo - teorija i praksa*, 26 (9-10), str. 36-43.
7. Bjelopoljak, A. (2012). *Pranje novca Sumnjive transakcije i Off shore zone*. JU „Gradska biblioteka“ , Kakanj
8. Bošković, G., (2005). *Pranje novca*. BeoSing, Beograd
9. Cindori, S. i Petrović, T. (2016). Indikatori rizičnosti bankarskog sektora u okvirima prevencije pranja novca. *Zbornik PFZ*, 66, (6) 761-784.
10. Cindori, S. (2010). Procjena stupnja rizika poreznih savjetnika u sustavu sprječavanja pranja novca. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci* 31 (2). str. 809-827.
11. Council of Europe, (2012). Moneywal report: criminal money flows on the internet: methods, trends and multi-stakeholder counteraction
12. Čudan, A. i Fijat, A., (2015). *Rizici i prevencija pranja novca – monografija,* Subotica, Printex, str. 62.
13. Daniali, G. (2014). E- money laundering Prevention. *New Marketing Research Journal*, 4, 29-38.
14. Direktivom 2005/60/EC Evropskog Parlamenta i Savjeta od 26. oktobra 2005 o sprečavanju korištenja finansijskog sistema u svrhu pranja novca i finansiranja terorizma.
15. Esoimeme, E. E., *The Risk-Based Approach to Combination Money Laundering and Terrorist Financing*, Eric Press, New York, 2015.
16. Fiedler, I. (2013). *Online gambling as a game changer to money laundering*? OnlineGamblingasaGameChangertoMoneyLaundering.pdf pristupljeno 27.06.2019.godine.
17. Filipkowski, W. (2008). Cyber laundering: an analysis of typology and techniques. Int. *J. Crim. Justice Sci*. **3** (1), 15–27
18. Gilmor, V. S., (2006). *Prljav novac, Razvoj međunarodnih mjera za borbu protiv pranja novca i finansiranja terorizma.* Prevod Mates, V., Izdanje Savjeta Evrope, „Plus“ Beograd.

19. Krivični zakon Bosne i Herceogivne Krivični zakon Bosne i Hercegovine (Službene glasnik Bosne i Hercegovine br. 03/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06 i 55/06, 8/10, 47/14, 22/15, 40/15, 35718),
20. Leko, V. (1998.). Financijsko okruženje marketinga, materijal za izučavanje na disciplini "Financijsko okruženje marketinga", Zagreb: Ekonomski fakultet Sveučilišta u Zagrebu, Specijalistički poslijediplomski studij "Upravljanje poslovnim-industrijskim marketingom"..
21. Madinger, J. (2012). *Money Laundering: Guide for Criminal Investigator.* Third Edition, CRC Press, Boca Raton.
22. Madsen, F. G. (2009), *Transnational organised crime*, Oxon: Routledge.
23. Meijerink, T. J. (2013). *Carding Crime Prevention Analysis.* Netherlands Police Agency, Universiteit Twente.
24. Meštrović, D., (2002), Legalizacija nelegalno stečenog kapitala. *Policija i sigurnost* 11 (2002), 1-3, str. 147.
25. Odluci o upravljanju informacionim sistemom u banci (2017). Agencije za bankarstvo Federacije Bosne i Hercegovine
26. Ollman, G. (2004). The Phishing Guide – Understanding and Preventing.*White Paper, Next Generation*. Security Software Ltd.
27. Polman, E, Effron, D. A. i Thomas, M. R. (2018). Other people's Money: Money's Perceived Purchasing Power is Smaller for Others for the Self. *Journal of Consumer Research,* 45 (1), 109-125.
28. Porobić, M i Bajraktarević, M. (2012). Cyber kriminal, pranje novca i finansijske istrage. Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa.
29. Savona, E. (2004), *Responding to Money Laundering: International Perspectives*, Harwood Academic Publishers, London, str. 153-154.
30. Savić, B. (2016). Money Laundering and Ways of Suppressing It In The Public Sector *Безбједност - Полиција* - Грађани, година XII број 1–2/16.
31. Siwi, Y. E, (2018) Mafia, money-laundering and the battle against criminal capital: the Italian case. *Journal of Money Laundering Control, Vol. 21 Issue:* 2, 124-133,
32. Vuksanović, E. (2006). *Elektronsko bankarstvo*, Beograd, Beogradska bankarska akademija, str. 218.
33. Yubin, M. (2003). *E-Banking: Status, Trends, Challenges and Policy Issues. CRBC Seminar*, The Development and Supervision of e-banking, Shangai.
34. Weaver, S. (2005). Modern day money laundering: does the solution exist in an expansive system of monitoring and record keeping regulations? Annu. Rev. Bank. *Law Financ. Law* **24**, 443–465
35. Weisman, M. F. 2014. *Money laundering legislation, regulation and enforcement,* American Bar Association, Chicago, , str. 5 – 6.
36. Villasenor, J., Bronk, C. i Monk, C. (2011). *Shadowy figures: tracking illicit financial transactions in the murky world of digital currencies, peer-to-peer networks, and mobile device payments.* Paper, The Brookings Institution and the James A. Baker III Institute for Public Policy

http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub FinancialTransactions-082911.pdf pristupljeno 30.06.2019.godine

37. Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti "Službeni glasnik BiH" br. 46/16.
38. Zirojević, A. (2017). Specifičnosti pranja novca u bankarskom sektoru. *PRAVO – teorija i praksa*, 7-9, 16-26.