Model rane detekcije sumnjivih bankovnih transakcija

Božić, Darjan

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij poslovne ekonomije, smjer Financije

Model rane detekcije sumnjivih bankovnih transakcija

Diplomski rad

Darjan Božić

Zagreb, veljača, 2023.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij poslovne ekonomije, smjer Financije

Model rane detekcije sumnjivih bankovnih transakcija

Model for early detection of suspicious bank transactions

Diplomski rad

Darjan Božić, 0067566554

Mentor: izv. prof. dr. sc. Lucija Rogić Dumančić

Zagreb, veljača, 2023.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.
Izjavljujem da nijedan dio rada / prijave teme nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada / prijave teme ne krši bilo čija autorska prava.
Izjavljujem, također, da nijedan dio rada / prijave teme nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student:

U Zagrebu, 14.2.2023 Dorjan Božić
(potpis)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.
I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.
I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

Student:

In Zagreb, 14.2.2023 Dorjan Božić
(signature)

Sažetak

Volumen oprane količine novca na svjetskoj se razini povećava, zbog čega razvitak novih načina otkrivanja pranja novca postaje prioritet. Ovaj rad nastoji na teorijskoj osnovi razviti model rane detekcije pokušaja pranja novca baziran na skupovima pravila koja procjenjuju sumnjivost bankovnih transakcija te funkcionalnu verziju opisanog modela testirati na generiranom skupu od 10.000 transakcija. Sumnjivim je označeno njih 119, a najčešći razlog za sumnju bili su iznosi iznad određene vrijednosti i transakcije sa rizičnim državama. Dodatno, istraženi su načini poboljšanja modela upotrebom rudarenja podataka i strojnog učenja, koje je u stanju analizirati ogromne količine povijesnih podataka, u njima uočiti uzorke i povezanosti i na temelju njih smjesta otkriti slične transakcije pranja novca, u trenutku njihovog izvršavanja, sa preciznošću do 90%.

Ključne riječi: pranje novca, transakcija, otkrivanje, model, strojno učenje

Abstract

The volume of laundered money is increasing worldwide, which is why development of new ways of detecting money laundering is becoming a priority. This work aims to, on a theoretical basis, develop a model for the early detection of money laundering attempts based on sets of rules that assess the suspiciousness of bank transactions and to test the functional version of the described model on a generated set of 10,000 transactions. 119 of them were marked as suspicious, and the most common reason for suspicion were amounts above a certain value and transactions with risky countries. Additionally, ways of improving the model were explored using data mining and machine learning, which is able to analyse immense amounts of historical data, spot patterns and connections in them and, based on them, immediately detect similar money laundering transactions, at the time of their execution, with a precision of up to 90 %.

Keywords: money laundering, transaction, detection, model, machine learning

Sadržaj

1. UVOD

1.1. Predmet i cilj rada

Razvoj modernog međunarodnog bankovnog sustava prate i novi načini pranja novca. Kriminalizirano je nedavno, a postoji još od antičkih vremena (Unger i van der Linde, 2013). Danas je prepoznato kao globalni problem s ozbiljnim ekonomskim i društvenim posljedicama zbog čega je istraživanje pranja novca i problematike koju donosi predmet ovog rada. Tradicionalne metodologije za otkrivanje pranja novca uključuju manualne provjere računalnih baza podataka, nadzor, presretanje pošte osumnjičenika, sudske pozive, razgovore sa suradnicima, naloge za pretragu i intervjue (Rocha-Salazar, 2021). U kontekstu stalno rastuće količine opranog novca iskazale su se nedostatnima. Pronalazak novih kreativnih rješenja za detekciju pranja novca u interesu je banke kao institucije, države te svakog pojedinca koji u njoj živi.

Razvoj kartičnog i internetskog plaćanja otvara nove načine za suočavanje s ovim problemom. Moderna tehnologija omogućuje bankovnim sustavima pohranjivanje informacija o svakoj izvršenoj transakciji u baze podataka te, posljedično, njihovu akumulaciju i analizu. Kad se na određenom skupu transakcija uspješno dokaže da su bile korištene u nekoj od faza pranja novca, moguće je uočiti ponavljajuće uzorke, povezanosti i kauzalnosti te ih dokumentirati. Iz takvih uzoraka moguće je doći do zaključaka, izdvojiti ih u skup pravila, a na temelju njih, zakona i literature napraviti sustave otkrivanja pranja novca. Današnje banke tako su razvile različite sustave koji ažurno provjeravaju svaku izvršenu transakciju pojedinca i šalju upozorenja u slučaju sumnje na pranje novca (Leite, 2019).

Cilj ovog rada je istražiti teoriju djelovanja ovakvih sustava, napraviti model i na temelju njega izraditi pojednostavljenu funkcionalnu verziju jednog sustava rane detekcije sumnjivih transakcija. Dodatno, opisan sustav će se testirati na generiranom skupu podataka, analizirati će se njegovo djelovanje te, konačno, sagledati mogući načini unaprjeđenja kroz korištenje modernih tehnologija.

1.2. Izvori i metode prikupljanja podataka

U izradi rada korišteni su relevantni akademski članci i knjige te publikacije institucija i uglednih poduzeća tematski povezani uz pranje novca u kombinaciji s internetskim bazama podataka za pristup ključnim statističkim podacima i indeksima koji uključuju Europol, FATF, UNODC, Mrežu za borbu protiv financijskog kriminala SAD-a, MMF, Eurostat, OECD,

Hanfa-u, Swift, ECB, Mrežu za poreznu pravdu (engl. *Tax Justice Network*), Nacionalnu komisiju za infrastrukturu Ujedinjenog kraljevstva, Ministarstvo financija RH i SEON.

1.3. Sadržaj i struktura rada

Rad je podijeljen na tri logičke cjeline. Prva se fokusira na opće karakteristike pranja novca i obrađuje tematiku povijesti pranja novca i relevantnih aktera, sam pojam i proces pranja novca, kao i trenutnu regulaciju tog područja. Slijedeća cjelina proučava suvremeni okvir provođenja bankovnih transakcija u vidu makroekonomskih determinanti razvoja internet bankarstva i načina izvršavanja transakcija plaćanja, na domaćoj i internacionalnoj razini. Konačno, posljednja cjelina prezentira sam model rane detekcije sumnjivih bankovnih transakcija, njegovo djelovanje, testiranje, identificirane nedostatke i načine unaprjeđenja kroz korištenje modernih tehnologija i saznanja.

2. KARAKTERISTIKE PRANJA NOVCA

2.1. Faze pranja novca

Cilj pranja novca je prikrivanje njegovog nezakonitog podrijetla. Riječ je o sekundarnom kaznenom djelu koje je povezano s drugom povredom zakona (Villányi, 2021). Izvori prihoda za perače novca široki su i uključuju gotovo sve vrste teških zločina. (Teichmann, 2019). Počinitelji pranja novca obično su trgovci drogom, pronevjeritelji, teroristi, korumpirani javni službenici, trgovci oružjem i drugi pojedinci s pristupom velikim količinama neprijavljene gotovine koju nastoje prikazati kao da je proizašla iz legitimnog poslovnog izvora (Seymour, 2008). Također, kaznena djela mogu biti različite vrste krađa, trgovina zabranjene robe, kao i druge nenasilne radnje poput porezne prijevare, podmićivanja te u današnje vrijeme sve relevantnije, kriminal preko interneta.

U slučajevima utaje poreza velikih razmjera, korupcije, transnacionalne trgovine drogom i sličnih organiziranih oblika kriminala, pranje novca može uključivati vrlo složene sheme koje se izvode u više zemalja. Pravno se gledište usredotočuje na četiri različite skupine aktivnosti: pretvorbu ili prijenos imovine iz njenog nezakonitog izvora, prikrivanje njenog nezakonitog podrijetla, stjecanje, posjedovanje i korištenje takve imovine te sve vrste sudjelovanja u nezakonitim radnjama povezanim s pranjem novca (Villányi, 2021).

Razmjere pranja novca teško je procijeniti, ali smatraju se značajnima. Procjene prije 2000-ih predlagale su da se godišnje u svijetu opere od 500 milijardi do jednog bilijuna američkih dolara (Baker, 1999), dok novije procjene trenutnu količinu pranja novca procjenjuju između 2 i 5% svjetskog BDP-a, što je između 800 milijardi i 2 bilijuna dolara svake godine (UNODC, 2022). Dokazi upućuju na to da većina malih prijestupnika sama pere novac, jednostavno zato što ne zarađuju toliko novca da bi im bio potreban stručnjak. Kradljivac ili niži diler droge plaćanjem stanarine ili računa za režije u gotovini u većini slučajeva ne izaziva nikakvu sumnju. Na višoj razini, iznose se može pomiješati sa legalnim prihodima tvrtke koja velikim dijelom koristi gotovinu, poput praonice rublja ili bara, dok se za složenije slučajeve koristi se model tri faze, široko prihvaćen okvir za analizu procesa pranja novca koji je predložio William Rosenblatt (Villányi, 2021).

Sheme pranja novca obično su kružne (UNODC, 2022), novac na kraju završi kod osobe s kojom je bio originalno. Prva je faza polaganja, odnosno, trenutak kada se sredstva pribavljena na nezakonit način upotrebom različitih metoda i tehnika odvajaju od svog pravog, nezakonitog izvora te se prvi put uvode u financijski sustav. Ona je ujedno i najrizičnija, jer je novac u

pitanju najpodložniji otkrivanju (HANFA, 2015). Nezakoniti prihod često se dijeli na više dijelova kako bi se zaobišli pragovi za prijavu. U nedostatku odgovarajućeg sustava nadzora, moguće je polagati manje iznose nekoliko puta u različitim poslovnicama banke, ostavljajući dojam da te transakcije nisu povezane. Često se koriste rođaci i prijatelji suučesnici, u mnogim slučajevima supruge ili djevojke počinitelja. Alternativno su to socijalno marginalizirane osobe s ekonomskim poteškoćama, koje nude svoje usluge u zamjenu za manji iznos, mnogi od kojih ne razumiju svoju ulogu u ilegalnoj aktivnosti ili svojevoljno zatvaraju oči pred njom (Villányi, 2021).

Druga je faza prikrivanja, koja podrazumijeva plasiranje sredstava u financijske tokove, kada se pomoću većeg broja složenih transakcija pokušava prikriti izvor nezakonito stečenih sredstava ili njihovog vlasnika (HANFA, 2015). Svaka slijedeća transakcija dodatno otežava otkrivanje originalnog izvora sredstava. U ovoj se fazi često koriste offshore tvrtke kao instrumenti prijenosa novca (Cindori, 2007).

Posljednja je faza integracije, u kojoj se novac uključuje u legalne financijske tokove i pripaja ostalim vrijednostima financijskog sustava zemlje, čime se gotovo onemogućava otkrivanje originalnog izvora sredstava (HANFA, 2015). Obično se cilja na pretežno gotovinske poslove, poput ugostiteljstva, turizma, zabave, prijevoza i građevinarstva, no također se koriste i radno intenzivne industrije s velikim brojem neprijavljenih radnika, dok se neki pojedinci odlučuju za opciju formalnog zapošljavanja sebe, rodbine i prijatelja na fiktivnim radnim mjestima (Villányi, 2021).

Neki od učinaka uspješno provedenih faza pranja novca su demotiviranje poštene poslovne aktivnosti, promjene u relativnim cijenama, štednji i proizvodnji kroz ulaganja nezakonito stečenog novca u sektore poput transportne industrije, restorana i stanovanja; utjecaji na likvidnost, ugled, integritet i stabilnost financijskog sektora države. Dodatno, javni sektor gubi porezne prihode, a kriminalni novac može poslužiti i za kupnju javnih poduzeća tijekom privatizacijskih napora države. Pojavljuju se i društveni i politički učinci poput povećane korupcije i mita. Naime, politički dužnosnici, odvjetnici, javni bilježnici, agenti za nekretnine, računovođe i revizori mogu postati suučesnici budući da su za pranje novca potrebni pomagači, čime potkopavanje rada institucija također postaje mogućnost. Ove učinke teško je izolirati i promatrati ih izravno, što predstavlja problem za regulaciju. Suvremeni kontekst deregulacije financijskih tržišta i slobodnog kretanja kapitala između zemalja pranje novca čini globalnim fenomenom (Unger i van der Linde, 2013).

2.2. Povijest pranja novca

Pranje novca počelo se smatrati kriminalom 1980-ih (Seymour, 2008). Prije toga je u fokusu jedino bio zločin u pozadini, a ne samo korištenje novca zarađenog preko zločina (Muller, Kalin, Goldsworth, 2007). Pranje novca svoje ime duguje Al Capone-u, koji je za prikrivanje ilegalnih prihoda od alkohola tijekom prohibicije 1930-ih u SAD-u koristio praonice rublja. Praonice rublja su se u okolnostima kada gotovo nijedno kućanstvo nije imalo perilicu, iskazale kao idealno mjesto za ubacivanje novca od ilegalne prodaje alkohola u sustav radi velikih količina gotovine koji je prolazio kroz njih (Unger i van der Linde, 2013). Naime, novac dobiven ilegalnim prodavanjem alkoholnih pića bi se stavljao u blagajnu praonice, lažno tvrdeći da dolazi od legalne djelatnosti (Villányi, 2021). No, pranje novca kao takvo postoji i prije toga, te je jedna od najstarijih poznatih tehnika za izbjegavanje vladinog nadzora bila uporaba međunarodne trgovine za prikriven prijenos novca iz jedne zemlje u drugu, putem sredstava lažnog fakturiranja ili lažnog deklariranja robe (Unger i van der Linde, 2013).

Prva dobro dokumentirana uporaba izraza pranja novca datira iz skandala Watergate, iz 1973., kad je velika količina gotovine položena u meksičke banke, pa kasnije prebačena natrag u Sjedinjene Države, čime se skrivalo podrijetlo novca i identitet donatora koji su financirali tadašnju republikansku kampanju (Villányi, 2021 prema Rosenbaum, 1974). Iako pranje novca već dugo postoji, kao istaknuto pitanje nacionalne i međunarodne sigurnosti koje je potrebno regulirati pojavljuje se tek nakon neuspješnih napora da se smanji trgovina drogom 1980-ih, te nakon skandala 9/11. Naime, u nemogućnosti da se dođe do dilera droge i drugih kriminalaca izravno, pokušalo ih se spriječiti da koriste novac zarađen kroz kriminalna djela (Unger i van der Linde, 2013).

Godine 1986. SAD je postala prva zemlja koja je pranje novca proglasila ilegalnim, s kaznama do 20 godina zatvora i 500.000 dolara novčane kazne. Razvio se popis zločina preduvjeta za pranje novca. Izvorno su to uglavnom bili zločini povezani s drogom, dok su naknadno dodavani krivotvorenje, prijevare, ilegalni rad, a poslije skandala 09/11 i financiranje terorizma (Unger i van der Linde, 2013).

Tradicionalne metodologije za otkrivanje pranja novca i financiranja terorizma uključuju manualne provjere računalnih baza podataka, nadzor, presretanje pošte osumnjičenika, sudske pozive, razgovore sa suradnicima, naloge za pretragu i intervjue. Mnoge od ovih tehnika su ručne, što ih čini skupim i neučinkovitima, zbog čega su financijske institucije razvile sustave za otkrivanje sumnjivih transakcija na temelju fiksnih pravila koja podliježu određenim pragovima (Rocha-Salazar, 2021.) temeljenim na propisima.

Na taj način se provođenje zakona oslanjalo na privatni sektor koji je izvještavao javne agencije u slučaju detektiranja pranja novca. U SAD-u su banke morale podnositi izvješća o gotovinskim transakcijama u valuti koje premašuju 10.000 dolara. Regulacija temeljena na pravilima bila je manje rizična i za privatni sektor i za državu. Budući da su postojali eksplicitni kriteriji za prijavu, provjera transakcija je bila standardni postupak otkrivanja pranja novca. Bankovna izvješća su provjeravana naknadno (Unger i van der Linde, 2013). Međutim, javni karakter regulacije temeljene na pravilima pokazao je određene nedostatke, pošto su kriteriji bili javni, perači novca su mogli razviti načine kako ih zaobići, primjerice na način da velike depozite podijele na manje iznose kako bi ih držali ispod praga za prijavu (Takats, 2007).

Naknadno je zaključeno da pristup temeljen samo na pravilima potiče pretjerano izvještavanje, zbog čega su SAD, a kasnije i Europa prešli s pristupa temeljenog samo na pravilima na pristup temeljen i na riziku. Privatnim akterima je dano više diskrecije o tome što trebaju prijaviti i rečeno im je da prijavljuju transakcije koje smatraju sumnjivima, što je značilo da privatni akteri moraju samostalno procjenjivati rizike transakcija, no, također i da su izloženi opasnosti da budu optuženi za lažno prijavljivanje (Unger i van der Linde, 2013).

Budući da je pranje novca uglavnom bio problem za bogate zemlje, svjestan međunarodne dimenzije problema, SAD je izvršio pritisak na zemlje G-7 grupacije da osnuju organizaciju koja bi koordinirala borbu protiv pranja novca, pa je 1989. godine osnovana Grupa za financijsku akciju protiv pranja novca (engl. *Financial Action Task Force* - FATF) (Unger i van der Linde, 2013). Svrha FATF-a je postavljanje standarda i promicanje učinkovite provedbe zakonskih, regulatornih i operativnih mjera za borbu protiv pranja novca, financiranja terorizma i drugih povezanih prijetnji na cjelovitost međunarodnog financijskog sustava. Redovito objavljuje i ažurira okvir mjera koje bi zemlje trebale provoditi u cilju borbe protiv pranja novca (FATF, 2022).

U nedostatku pravnih instrumenata koji bi natjerali države ne-članice da slijede njegova pravila, FATF se oslanjao na diplomaciju, recenzije te svoju crnu listu zemalja iz 2000. godine koje su se smatrale tolerantnima prema pranju novca. Činjenica da danas nijedna zemlja nije ostala na crnoj listi sugerira da su se sve zemlje djelomično popravile i prilagodile njihov regulatorni okvir za borbu protiv pranja novca (Unger i van der Linde, 2013).

Pranje novca danas se indirektno nalazi na prvom mjestu na listi prioriteta Europske multidisciplinarne platforme protiv kriminalnih prijetnji (engl. *European Multidisciplinary Platform Against Criminal Threats, EMPACT*). EMPACT navodi da mu je u periodu 2022. do 2025. godine prioritet identificirati i prekinuti visokorizične kriminalne mreže aktivne u

Europskoj uniji, poput mafijaških, etničkih, obiteljskih organizacija i drugih strukturiranih mreža pojedinaca, s posebnim naglaskom na kriminalne mreže koje potkopavaju vladavinu prava kroz korupciju, nasilje, zastrašivanje i pranje svojih kriminalnih prihoda kroz paralelni podzemni financijski sustav (Europol, 2022).

U 2020. godini, EMPACT je u sklopu operacije EMMA pokrenuo 1.529 kriminalističkih istraga, u kojim je sudjelovalo više od 500 banaka i financijskih institucija te je identificirano preko 6.809 korisničkih računa koji su se koristili za transferiranje imovine, a uhićeno je 455 osoba. Kroz cijelu 2020. godinu, u sklopu borbe protiv pranja novca zaplijenjeno je 19.829.888 eura u gotovini, 118 bitcoina, 4 nekretnine i 5,5 milijuna eura u zlatu i srebru (Empact, 2021). Uzevši u obzir najnižu procjenu ukupnog iznosa opranog novca na svjetskoj razini od 656 milijardi eura (UNODC, 2022), zaplijenjen iznos EMPACT-a čini 0,0030% (preračunato iz američkog dolara prema prosječnom tečaju za 2022. godinu).

2.3. Sustav regulacije pranja novca u RH

Relevantna međunarodna regulativa iz područja pranja novca i financiranja terorizma u Hrvatskoj obuhvaća:

- Konvenciju o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenoga kaznenim djelom
- Europsku konvenciju o suzbijanju terorizma
- Protokol o izmjenama i dopunama Europske konvencije o suzbijanju terorizma
- Konvenciju Vijeća Europe o sprječavanju terorizma
- Konvenciju Vijeća Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenoga kaznenim djelom i o financiranju terorizma
- Međunarodnu konvenciju o suzbijanju financiranja terorizma
- Rezoluciju Vijeća sigurnosti Organizacije Ujedinjenih naroda br. 1373
- Konvencije Ujedinjenih naroda
- Preporuke međunarodne organizacije FATF o pranju novca i financiranju terorizma (HANFA, 2015)

Europska Unija je implementirala preporuke FATF-a donošenjem direktiva koje države članice moraju integrirati u nacionalno pravo, a time i Hrvatska. Prva Direktiva predviđa potrebu da financijske i kreditne institucije identificiraju i prijave sve sumnjive transakcije u svrhu sprječavanja korištenja financijskog sustava u svrhu pranja novca. Druga je proširila djelokrug prve na dodatne skupine, odnosno na trgovce automobilima, prodavače brodova, umjetnina,

antikviteta, zlata, srebra i nakita, a naknadno i na odvjetnike, javne bilježnike, porezne savjetnike, računovođe i agente za kupoprodaju nekretnina. Treća je u definiciju pranja novca uključila i financiranje terorizma te navodi da svaki pojedinac koji ulazi ili izlazi iz EU-a i nosi gotovinu u vrijednosti od 10.000 eura i više mora prijaviti taj iznos nadležnim tijelima države članice (Unger i van der Linde, 2013), bez obzira obavlja li se transakcija u obliku jedne operacije ili više njih.

Najnovija Direktiva iz 2015. godine naglašava važnost igara na sreću u kontekstu pranja novca i nalaže da se primjene mjere dubinske analize za transakcije u iznosu od 2.000 eura i više (Direktiva Europskog parlamenta i vijeća o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, 2015). Unutar tih okvira, svaka država članica slobodna je odrediti vlastiti pristup u borbi protiv pranja novca na način koji smatra primjerenim (Eurostat, 2013).

Uključivanjem u međunarodne financijske tokove, država je izložena ne samo pravnim ulaganjima, već i transakcijama s nepoznatim izvorima novca i identitetima osoba koje stoje iza transakcije (Cindori, 2007). Zato se propisuju mjere pojačane dubinske analize koje se trebaju primijeniti kada pojedinci posluju s partnerima koji dolaze iz visokorizičnih trećih zemalja, koje utvrđuje Komisija na temelju informacija relevantnih međunarodnih organizacija i stručnjaka, uključujući javne izjave FATF-a, nalaze evaluacija, objavljenih izvješća i slično (Pezer Blečić, 2014).

U Hrvatsko pravosuđe se navedene Direktive implementiraju Zakonom o sprječavanju pranja novca i financiranja terorizma, koji propisuje mjere, radnje i postupke koje obveznici i nadležna državna tijela moraju poduzimati u svrhu sprječavanja i otkrivanja pranja novca i financiranja terorizma. Propisuje se pojedinačna obveza obveznika za sastavljanje liste indikatora za prepoznavanje sumnjivih transakcija i osoba u vezi s kojima postoje razlozi za sumnju na pranje novca (HANFA, 2015). Prema članku 81. Zakona, nadležna tijela su Hrvatska agencija za nadzor financijskih usluga, Hrvatska narodna banka, Financijski inspektorat i Porezna uprava. Svi podaci prikupljeni u skladu s ovim Zakonom su povjerljivi te se mogu koristiti samo za otkrivanje i sprječavanje pranja novca i kaznenih djela povezanih s pranjem novca (Cindori, 2007).

Središnja nacionalna financijsko obavještajna jedinica zadužena za primanje obavijesti o sumnjivim transakcijama i provođenje operativnih analiza je Ured za sprječavanje pranja novca. Ured također sastavlja godišnje izvješće u kojem objavljuje broj sumnjivih transakcija zaprimljenih od banaka i drugih obveznika, broj inicijativa sa sumnjom na pranje novca

zaprimljenih od državnih tijela i inozemnih financijsko-obavještajnih jedinica, broj otvorenih predmeta sa sumnjom na pranje novca, broj blokada sumnjivih transakcija, kao i statističke podatke o međuinstitucionalnoj i međunarodnoj suradnji.

Kad zaprimi obavijest o sumnjivoj transakciji, Ured ima ovlaštenje privremeno zaustaviti njeno provođenje te može naložiti obvezniku (banci i dr.) da trajno prati transakcije sumnjive stranke u pitanju. Vrijednost naloga za privremeno zaustavljanje obavljanja sumnjivih transakcija u 2020. godini iznosila je 33.863.207 HRK, tj. 4.495.255 EUR (izračunato prema srednjem tečaju HRK/EUR za 2020. godinu prema HNB-ovoj tečajnoj listi, 7,5331) (Ministarstvo financija, 2021.).

Kako bi primorali obveznike na provođenje zakona, nadležna tijela na raspolaganju imaju administrativne mjere i sankcije koje se propisuju na temelju ozbiljnosti i trajanja prekršaja, stupnja odgovornosti pravne ili fizičke osobe, njihove financijske snage, koristi proistekle iz kršenja, odnosno gubitka treće strane (ako se može utvrditi), razine suradnje s nadležnim tijelom te ranije (ne)osuđivanosti odgovornih osoba. Sankcije se primjenjuju u slučaju neprovođenja dubinske analize stranaka i evidencije, neprijavljivanja sumnjivih transakcija te neprovođenja unutarnje kontrole.

U navedenim slučajevima kršenja obveza primjenjuje se minimum administrativnih mjera i sankcija koji uključuje: javnu izjavu u kojoj se utvrđuje fizička ili pravna osoba odgovorna za kršenje, nalog kojim se fizičkoj ili pravnoj osobi nalaže da prestane s takvim postupanjem i da ga ne ponovi, povlačenje ili suspenzija odobrenja za obavljanje upravljačke dužnosti i rad kod obveznika, te novčane sankcije koje su barem dvostruko veće od iznosa koristi proizašle iz kršenja, ako se ta korist može utvrditi u iznosu, a najmanje 1.000.000 eura. Kod kreditnih i financijskih institucija primjenjuju se i veće sankcije, najmanje 5.000.000 eura ili 10% ukupnog godišnjeg prihoda (Pezer Blečić, 2014).

2.4. Uloga poreznih oaza

Porezne oaze jurisdikcije su s niskim porezima koje tvrtkama i pojedincima nude prilike za izbjegavanje poreza. Porezne oaze u svijetu su male, imućne i dobro politički vođene, u njima stanuje oko 0.8% svjetske populacije. Privlače neproporcionalno velike udjele izravnih ulaganja svijeta zbog čega su njihova gospodarstva porasla mnogo brže od ostatka svijeta u proteklih 25 godina (Hines, 2007). Imaju vrlo nisku ili nultu poreznu stopu što ih čini privlačnima pojedincima koji žele izbjeći plaćanje poreza. Često su tajnovite i odbijaju suradnju s drugim jurisdikcijama, posebno u pogledu razmjene informacija (Mugarura, 2017), a također

ih karakteriziraju razvijene financijske institucije i tržišta, nedostatak transparentnosti te nedefinirana pravila i zakoni protiv pranja novca.

Za otvaranje računa u poreznoj oazi nije potrebno prebivalište pojedinca ili poslovna prisutnost u zemlji. Ulaganja u njih su sigurna, a njihove pojedinosti rijetko javne. Dodatnim proširenjem definicije, u porezne oaze se svrstava svaka međunarodna lokacija i offshore centar koji ima posebne porezne zakone za privlačenje kapitalnih ulaganja (Gyeni-Boateng, 2020). Danas u svijetu postoji otprilike 45 velikih poreznih oaza. Primjeri uključuju Andoru, Irsku, Luksemburg i Monako u Europi, Hong Kong i Singapur u Aziji, te Kajmanske otoke, Nizozemske Antile i Panamu u Americi (Hines, 2007).

Ulaganje u poreznu oazu ili preseljenje središta tvrtke u nju nije kazneno djelo, no one znaju biti mjesto gdje kriminalci peru svoj nezakonito stečen novac jer nude brojne pogodnosti ulagačima koji nisu voljni otkriti podrijetlo svoje imovine. Radi financijske tajnovitosti, one učinkovito štite ulagače od istraga i kaznenih progona iz njihovih matičnih zemalja (Gyeni-Boateng, 2020).

Pojedince i tvrtke koji djeluju i posluju u poreznim oazama trebalo bi klasificirati kao visokorizične i pri poslovanju s njima provesti pojačanu dubinsku analizu. Financijske transakcije trebale bi biti ispravno dokumentirane i pregledane, a u slučaju sumnje na pranje novca, podnijeto izvješće. Institucije koje se bave klijentima koji posluju i ulažu u porezne oaze, trebali bi uspostaviti sustave koji će im omogućiti dobivanje potrebne dokumentacije za identifikaciju kupaca, obradu transakcija te njihovu pohranu za buduću upotrebu, analizu i nadzor u suradnji s regulatornim tijelima (Gyeni-Boateng, 2020).

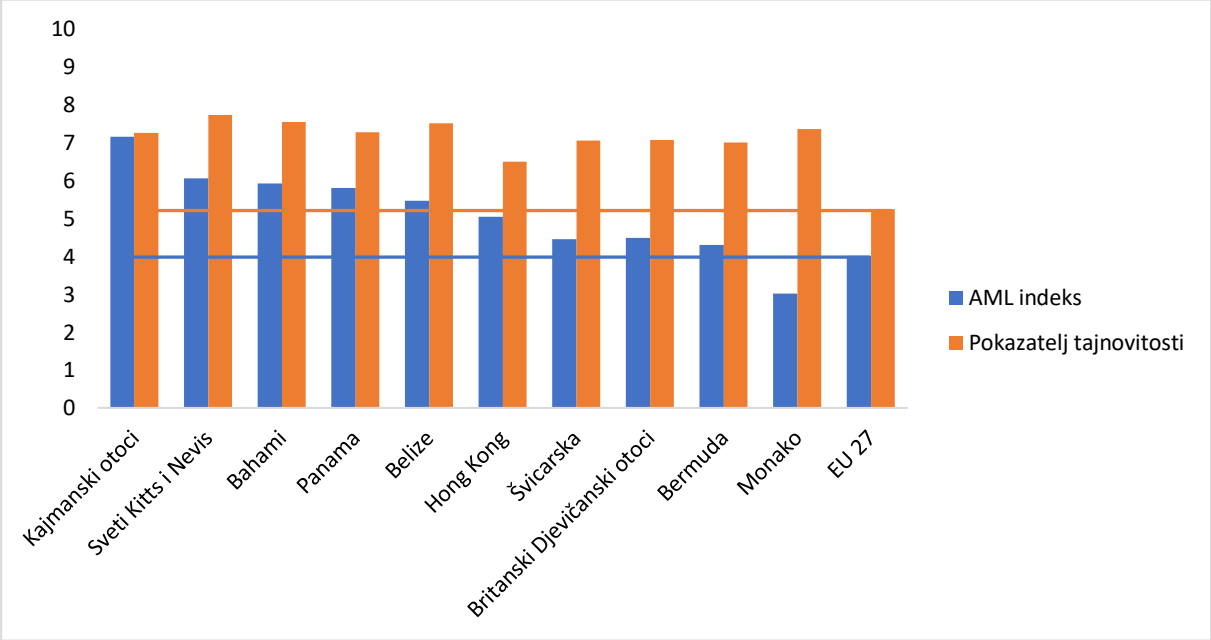
Prepoznaje se potreba za usklađivanjem međunarodnih poreznih zakona i zakona protiv pranja novca radi ukidanja regulatornih rupa u zakonima koje porezne oaze čine privlačnima za perače novca i korumpirane političke vođe u svijetu. Postoji bliska korelacija između zakona o bankovnim tajnama u offshore financijskim centrima i rasta financijskih zločina poput utaje poreza i pranja novca diljem svijeta (Mugarura, 2017).

U nastavku se prikazuju rezultati AML (engl. *anti-money-laundering*) indeksa i pokazatelja financijske tajnovitosti (engl. *secrecy score*) pojedinačnih država prilagođenih za ljestvicu od jedan do deset, s prosjekom zemalja europske unije kao referentnom vrijednošću (graf 1.). Baselov AML indeks mjeri rizik od pranja novca i financiranja terorizma u jurisdikcijama svijeta, ocjenjuje rizike na temelju podataka iz javno dostupnih izvora kao što je FATF, Transparency International, Svjetska banka i Svjetski ekonomski forum. Fokusira se na pet relevantnih domena, koje su:

- kvaliteta AML okvira
- mito i korupcija
- financijska transparentnost i standardi
- javna transparentnost i odgovornost
- pravni i politički rizici (Basel Institute on Governance, 2022).

Dalje, u rezultat financijske tajnovitosti ulaze analize pravnog okvira zemlje, njezinih zakona, propisa i provedbe. Pokazuje potencijal iskorištavanja određenog pravnog okvira za vlastitu korist (Tax Justice Network, 2018).

Graf 1. AML indeks i pokazatelj tajnovitosti odabranih poreznih oaza i prosjeka EU



Izvor: Izrada autora prema Basel Institute on Governance i Tax Justice Network, 2022.

Analizom podataka iz grafa 1. vidljivo je da svih deset promatranih poreznih oaza imaju viši pokazatelj tajnovitosti od prosjeka Europske unije, koji iznosi 5.2 boda, usporedno s najvišim rezultatima koji se odnose na Nevis (7,7), Belize (7,5), Monako (7,4) i Kajmansko otočje (7,3). Najbolji rezultat ima Hong Kong sa 6,5, što je i dalje 1,25 bodova više od prosjeka Europske unije. S druge strane, sveobuhvatniji AML indeks je viši od prosjeka zemalja europske unije (4,01) u svim promatranim državama osim Monaka, koje čine 90% promatranog uzorka. Najveći je na Kajmanskom otočju (7,16), Nevisu (6,06), Bahamima (5,93), Panami (5,81) i Belize-u (5,47), poreznim oazama koncentriranim oko Karipskog mora, a slijede ih Hong Kong sa 5,05 bodova i Švicarska sa 4,45.

Švicarska je nedavno signalizirala promjenu u svom stavu prema zakonima o bankovnim tajnama i naznačila da je je spremna prestati djelovati kao sigurno utočište za nezakonito bogatstvo korumpiranih političkih vođa, u suradnji s OECD-om bi trebala početi dijeliti dio podataka sa 60 drugih zemalja (Mugarura, 2017), što indicira početak promjena, no Bazelski institut za rukovođenje općenito zaključuje da oko poreznih oaza, a i svijeta općenito, ne vidimo dovoljan napredak u borbi protiv pranja novca.

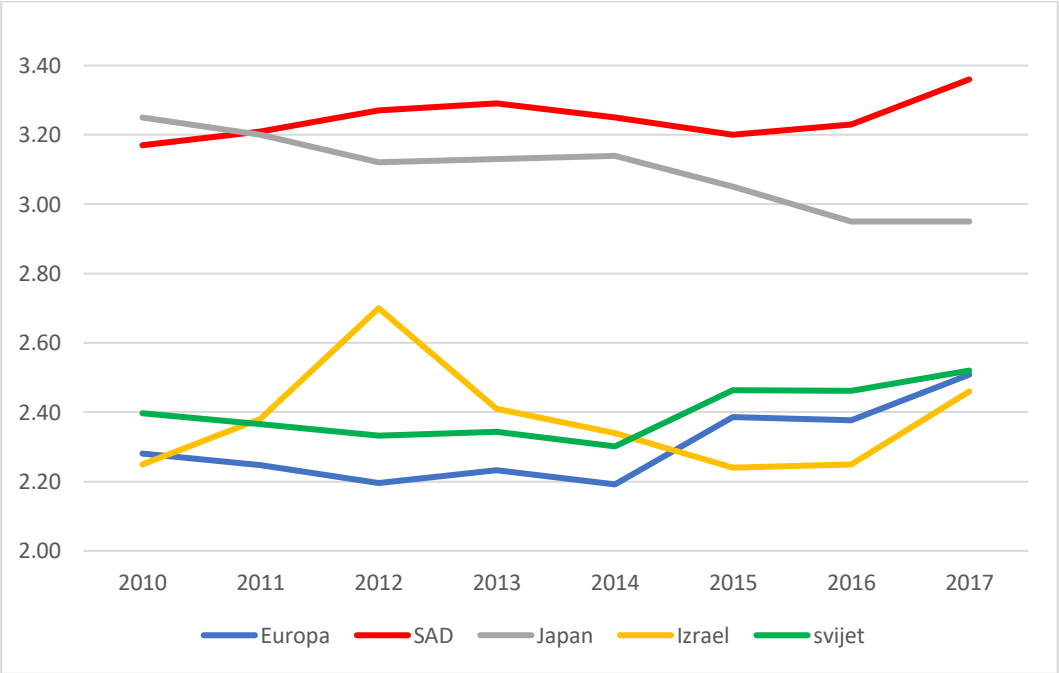
3. SUVREMENI OKVIR PROVOĐENJA BANKOVNIH TRANSAKCIJA

3.1. Makroekonomske determinante razvoja internet bankarstva

Internetsko bankarstvo pojam je koji opisuje digitalizaciju cjelokupnih bankovnih procesa. Realizira se putem ponude proizvoda i usluga preko interneta. Korisnicima omogućuje izvršavanje transakcija i pristup bankarskim uslugama putem uređaja, preglednika ili aplikacija, u bilo koje doba dana, neovisno o lokaciji korisnika usluge. Potreba za internet bankarstvom proizlazi iz sve veće potražnje kupaca za pristup i upravljanje njihovim financijskim podacima (Digital adoption, 2022).

Usvajanje internet bankarstva, odnosno stopa kojom potrošači, tvrtke i organizacije usvajaju usluge digitalnog bankarstva ovisi o preferencijama potrošača, konkurenciji u industriji, tehnološkom napretku i infrastrukturi, regulatornim zahtjevima, marketinškim strategijama, partnerstvima s pružateljima usluga i poboljšanju korisničkog iskustva(Digital adoption, 2022). Modeli digitalnog bankarstva prešli su iz jednostavnih oblika podrške stvarnoj fizičkoj posjeti poslovnici banke u kompletnu samostojeću alternativu.

Graf 2 Ulaganja u informatički i komunikacijski (ICT) sektor, % BDP-a



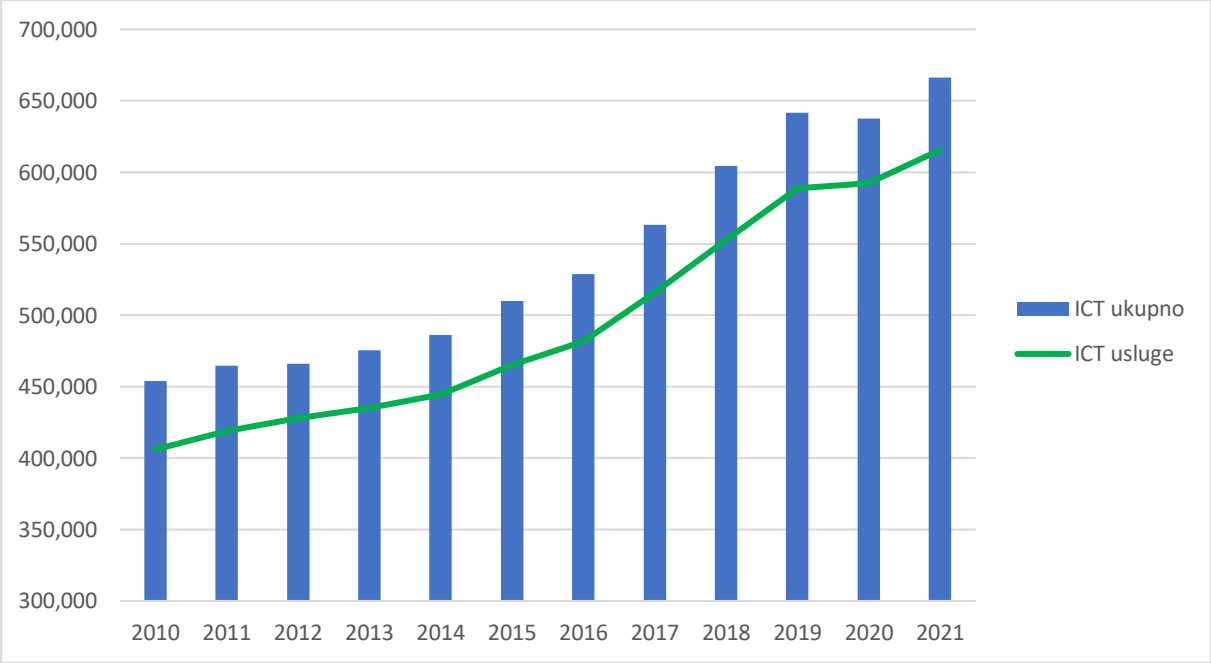
Izvor: izrada autora prema OECD Going Digital Toolkit, 2022.

Hunady, Pisar i Durcekova navode da su tvrtke u informatičkom sektoru važan izvor inovacija u gospodarstvu i da čine značajan udio ukupnih izdataka za istraživanje i razvoj u većini

europskih zemalja, najviše u nordijskim kao što su Island, Norveška i Finska. Zaključuju da ulaganja u istraživanje i razvoj imaju pozitivan učinak na pokazatelje poslovne uspješnosti, konkretno, produktivnost rada i dodanu vrijednost. U grafu 2. prikazana su ulaganja u informatički i komunikacijski sektor relevantnih geografskih cjelina i zemalja. Vidljivo je da SAD ima najviše udjele ulaganja u promatranom periodu, slijedi ga Japan, dok su ispod njega europske zemlje i Izrael. Promatrajući podatke na svjetskoj razini, uočljiv je trend povećanja ulaganja u informatički i komunikacijski sektor, sa 2,4% BDP-a u 2010. godini na 2,52% u 2017. godini.

Ukupna dodana vrijednost informatičkog i komunikacijskog sektora EU-a iznosila je više od 650 milijardi eura u 2021., od čega su najveći udio činile usluge, dvanaest puta veći od proizvodnje. Dodana vrijednost informatičkog sektora rasla je u cijelom periodu od 2010. do 2021. godine (graf 3.).

Graf 3 Dodana vrijednost informatičkog sektora (milijuni EUR), EU

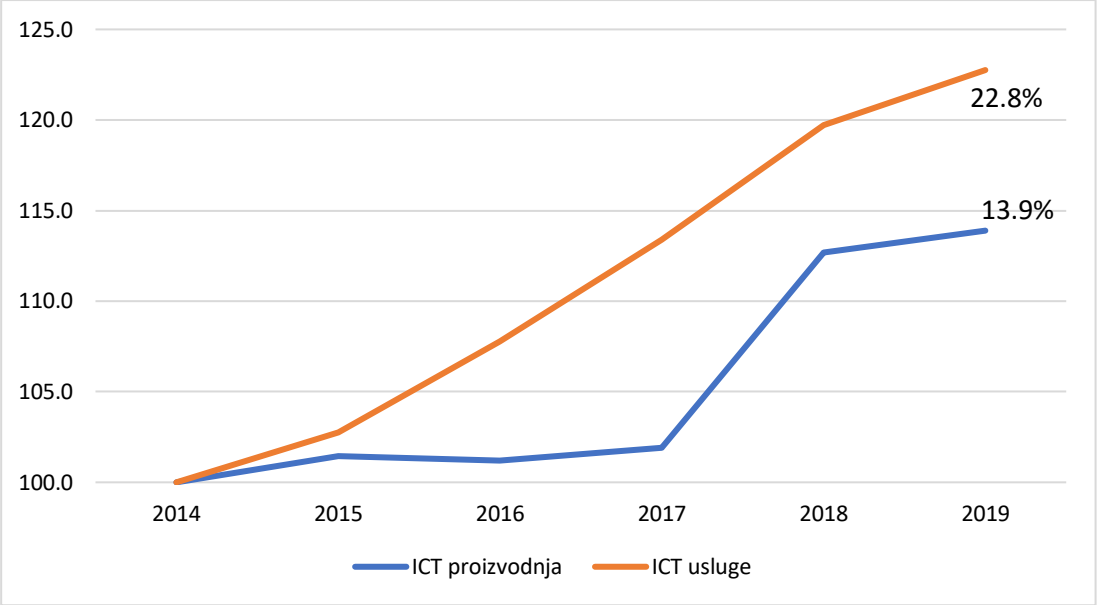


Izvor: izrada autora prema Europska Komisija, 2022.

Rast informatičkog sektora vidljiv je i kroz zaposlenost, koja ja u od 2014. godine do 2019. godine rasla za 22,8% u proizvodnji, te 13,9% u uslugama, u kojima je i internet bankarstvo, graf 4. Usluge su u promatranom periodu imale kontinuiran rast, dok je proizvodnja doživjela skok u 2017. godini. Dodatno, u 2019. najveći podsektor informatičkih usluga u EU, 'Računalno programiranje, savjetovanje i srodne djelatnosti', u kojem su i usluge internet bankarstva,

zapošljavao je deset puta više ljudi od najvećeg podsektora informatičke proizvodnje, 'Elektroničke komponente i ploče'. Informatički i komunikacijski sektor EU-a na kraju 2019. godine ukupno je zapošljavao preko 5,8 milijuna ljudi (Eurostat, 2022).

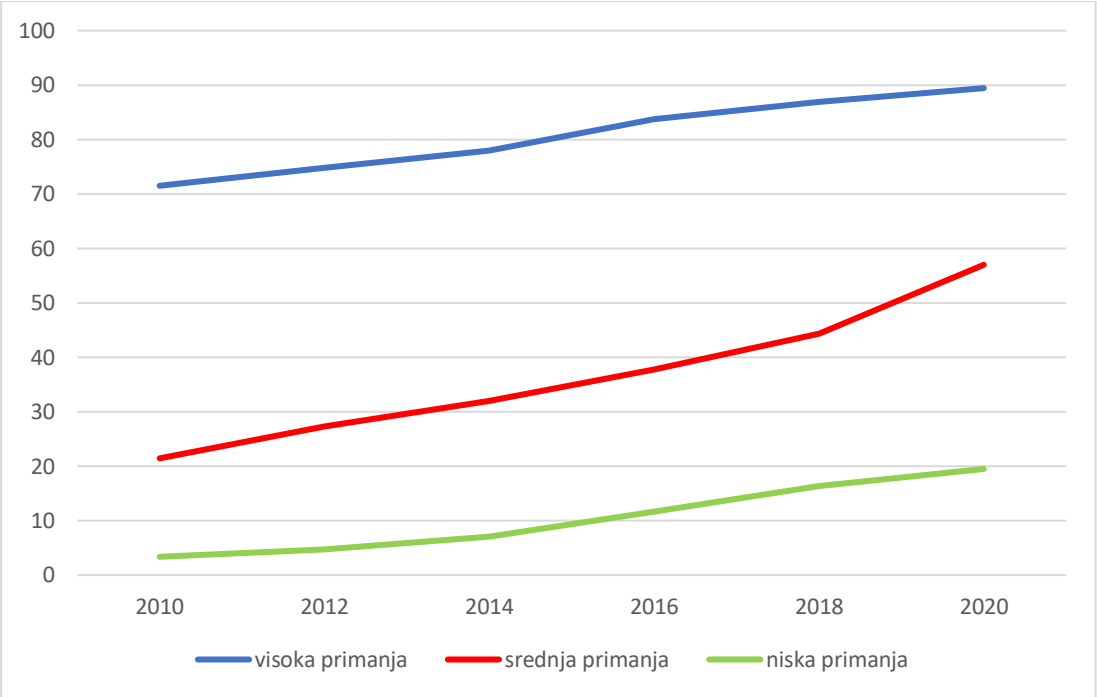
Graf 4 Zaposlenost u informatičkom sektoru, EU, 100 = 2014



Izvor: izrada autora prema Europska Komisija, 2022.

Nadalje, u grafu 5. prikazani su postoci populacije svijeta koji su imali pristup i koristili internet u periodu od 2010. do 2020. godine, raspodijeljeni prema njihovim primanjima.

Graf 5 Pojedinci koji koriste internet u svijetu (% stanovništva)

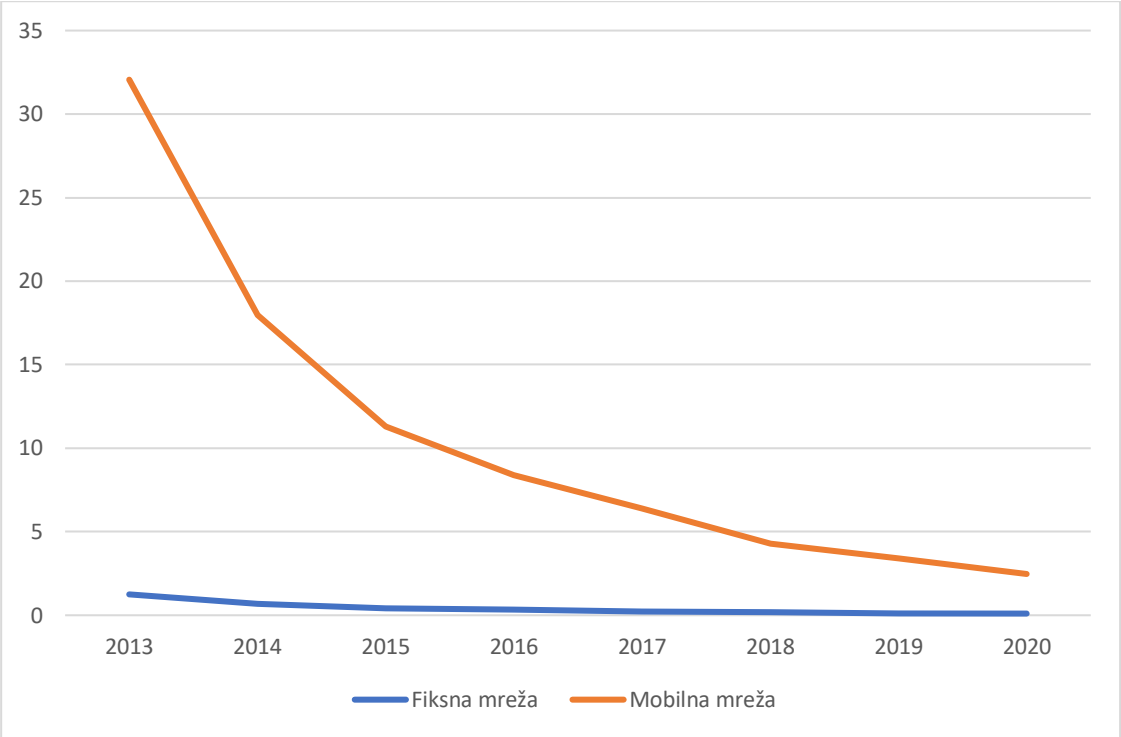


Izvor: izrada autora prema OECD, 2022.

Pod niža primanja ubrajaju se pojedinci s neto prihodom manjim od 50% medijana prihoda ukupnog stanovništva, srednja primanja podrazumijevaju pojedince s neto dohotkom između 50 i 150% prosječnog dohotka, dok razred viših prihoda identificira pojedince s neto prihodom iznad 150% medijana srednjeg dohotka (OECD, 2020). Moguće je uočiti uzlazan trend za sva tri razreda u promatranom periodu, najveći za srednja primanja, koja bilježe porast sa 21% na 57%, odnosno 36 postotna boda. Slijedi razred visokih primanja, s porastom od 18 postotna boda, te razred niskih primanja s rastom od 16 postotna boda.

Uz općenit porast broja korisnika interneta, bilježi se i pojeftinjenje interneta kroz godine. Prema podacima za Ujedinjeno Kraljevstvo, trošak jednog gigabajta preko fiksne mreže u Ujedinjenom Kraljevstvu pao je sa 1,63 funte u 2012. na 0,1 funtu, dok je prosječni trošak jedinice preko mobilne mreže pao sa 32 funte u 2012. na manje od 3 funte u 2020. godini.

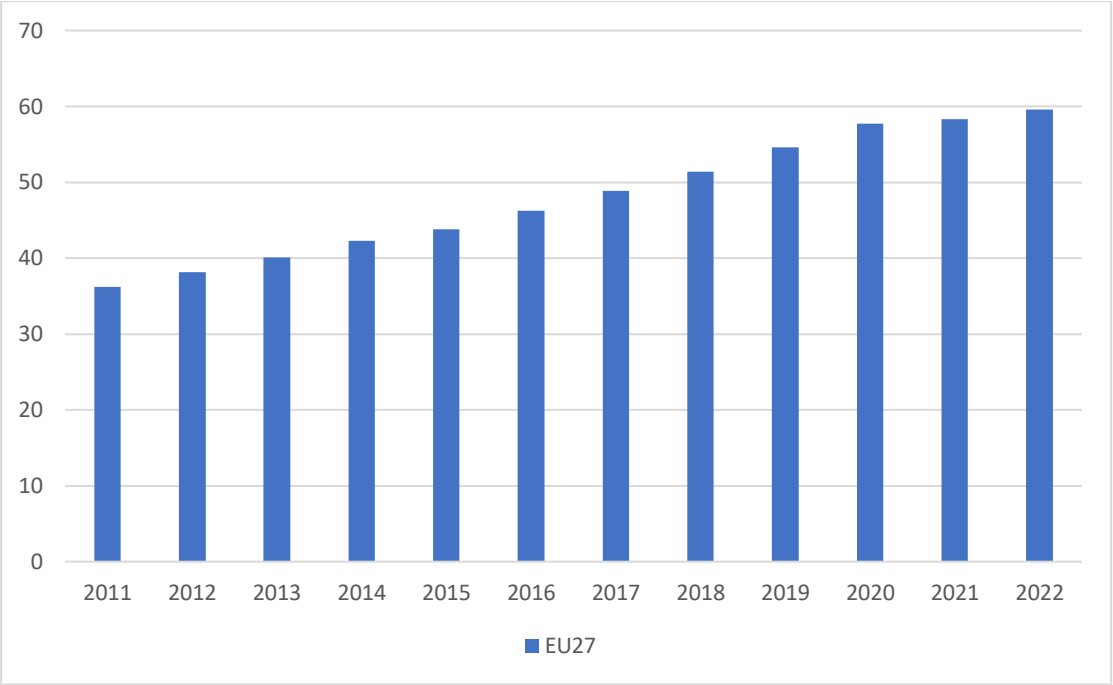
Graf 6 Troškovi jedinice internet podataka u UK, Gigabajti (izraženo u £)



Izvor: izrada autora prema National Infrastructure Commission, 2022.

Konkretan rast broja pojedinaca koji su koristili internet za internet bankarstvo kroz godine u EU prikazan je na grafu 7. Vidljivo je da u promatranom periodu dolazi do rasta od 23 postotna boda, sa 36% u 2011. na 60% u 2022. godini.

Graf 7 Pojedinci koji koriste internet za internet bankarstvo (% stanovništva)



Izvor: izrada autora prema Eurostat, 2022.

3.2. Internacionalna plaćanja kroz Swift

Plaćanja karticama prvi su put premašila plaćanja gotovinom u 2016. godini dosegnuvši 23 trilijuna dolara na globalnoj razini. Među razvijenim gospodarstvima, nordijske zemlje bilježe najviše stope bezgotovinskih plaćanja. U Švedskoj se gotovina koristi u samo 2% transakcija (Swift, 2022). U državama u razvoju, vlade obeshrabruju plaćanja gotovinom s ciljem povećanja transparentnosti i kontrole nad valutom. Prelazak na digitalna plaćanja stvara temeljne mogućnosti za prekogranične transakcije.

Internetska tržišta i platforme za online trgovinu, kao što su Uber, Amazon i Alibaba, mijenjaju tradicionalan proces kupnje. Uz njihove globalne poslovne modele, povijesno domaći kapitalni tokovi, kao što su taksi i kupnja hrane za van, postaju međunarodne transakcije. Moguće je uočiti trend povećanja udjela manjih transakcija u ukupnom broju prekograničnih transakcija. Prema Swiftu, broj prekograničnih transakcija u vrijednosti do tisuću dolara porastao je za 286% od 2017. do 2020. godine, raspon 1.000 do 10.000 porastao je za 163%, raspon 10.000 do 100.000 za 148%, a raspon 100.000 i više za 154% u istom vremenskom periodu od kraja 2017. do kraja 2020. godine.

Porast obujma međunarodnih plaćanja potiče banke da pronalaze nova tehnološka rješenja i poboljšaju postojeća kako bi zadovoljile potražnju. Kupci zahtijevaju nov, brz i digitalni standard usluge, uz istovremeno povećanje regulatornih zahtjeva međunarodnih standarda

plaćanja. Takva tehnološka rješenja zahtijevaju velika kapitalna ulaganja što favorizira velike banke, dok manjim bankama preostaje daljnje usmjeravanje na lokalno bankarstvo uz outsourcing aktivnosti poput internacionalnih plaćanja (Barbey et al., 2017).

Jedan od odgovora na rastuće potrebe internacionalnih plaćanja je neprofitna financijska institucija imenom Društvo za svjetsku međubankarsku financijsku telekomunikaciju (engl. *Society for Worldwide Interbank Financial Telecommunication*), skraćeno SWIFT. SWIFT čini ključni dio infrastrukture financijskih usluga i jedna je od najkorištenijih mreža u svijetu koju koristi preko dvjesto zemalja. Omogućava institucijama povezivanje i sigurno razmjenjivanje financijskih informacija preuzimajući posredničku ulogu.

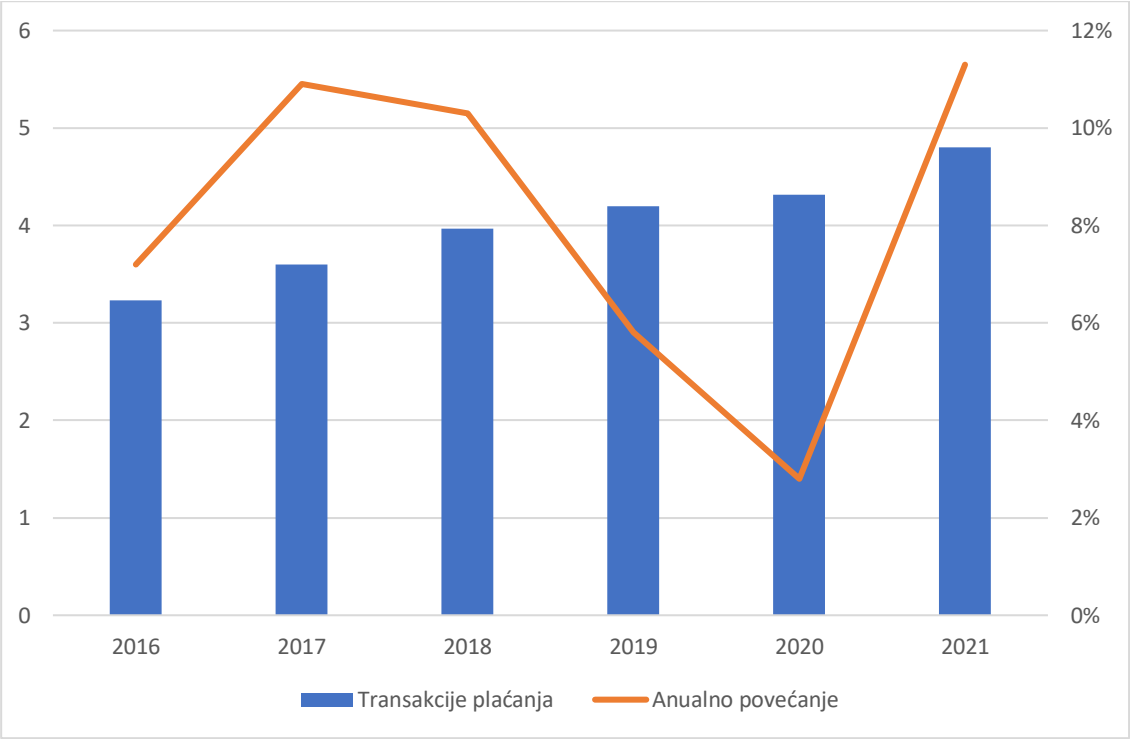
Reputacija SWIFT-a kao pouzdane temeljne infrastrukture financijskih usluga ne počiva na prijenosu imovine, već na vrijednosti koju financijska zajednica pridaje olakšanoj, brzoj i sigurnoj povezanosti. SWIFT je samo kanal za prijenos financijskih poruka, banke i klirinške kuće su te koje namiruju transakcije nakon što se priopći financijska uputa (Scott, Zachariadis, 2012).

SWIFT je osnovalo 239 banaka iz 15 različitih zemalja u 1970-ima radi smanjenja grešaka i povećanja učinkovitosti međubankovnih plaćanja (Seymour, 2008), u vrijeme kad je jedna prekogranična transakcija zahtijevala razmjenu više od deset poruka, što je proces činilo skupim i dugotrajnim, no SWIFT se brzo razvio u široku industrijsku kooperativu i postao mrežni fenomen. Počeci SWIFT-a leže u pronalaženju rješenja na probleme pristupa tržištu, transakcijske učinkovitosti, operativnog rizika, robusnosti i sigurnosti plaćanja, no on postupno preuzima odgovornost i za reguliranjem financijske infrastrukture te razvoja međunarodnih standarda plaćanja. U isključivom je vlasništvu svojih banaka članica i registriran u Briselu, a baza korisnika je naknadno proširena s banaka i na brokere, dilere, mjenjačnice, središnje depozitorije, klirinške kuće i međunarodne investicijske fondove (Scott, Zachariadis, 2012).

Danas 90% banaka i financijskih institucija koristi SWIFT kako bi olakšalo kretanje globalnog kapitala kroz bankarske sustave. Prosječno tranzitno vrijeme za provedbu transakcije je dvadeset sekundi (Seymour, 2008). SWIFT bilježi do 20,5 milijuna platnih transakcija dnevno, uz tendenciju rasta (Swift, 2022).

U cijeloj 2016. godini bilježio je 3,23 milijarde platnih transakcija te je uz prosječnu godišnju stopu rasta od 8,1% u periodu od 2016. do 2021. godine došao do 4,8 milijardi transakcija u 2021. Jedina godina u kojoj je rast bio manji od 5% je bila 2020., graf 8.

Graf 8 Broj transakcija plaćanja SWIFT-a, milijarde

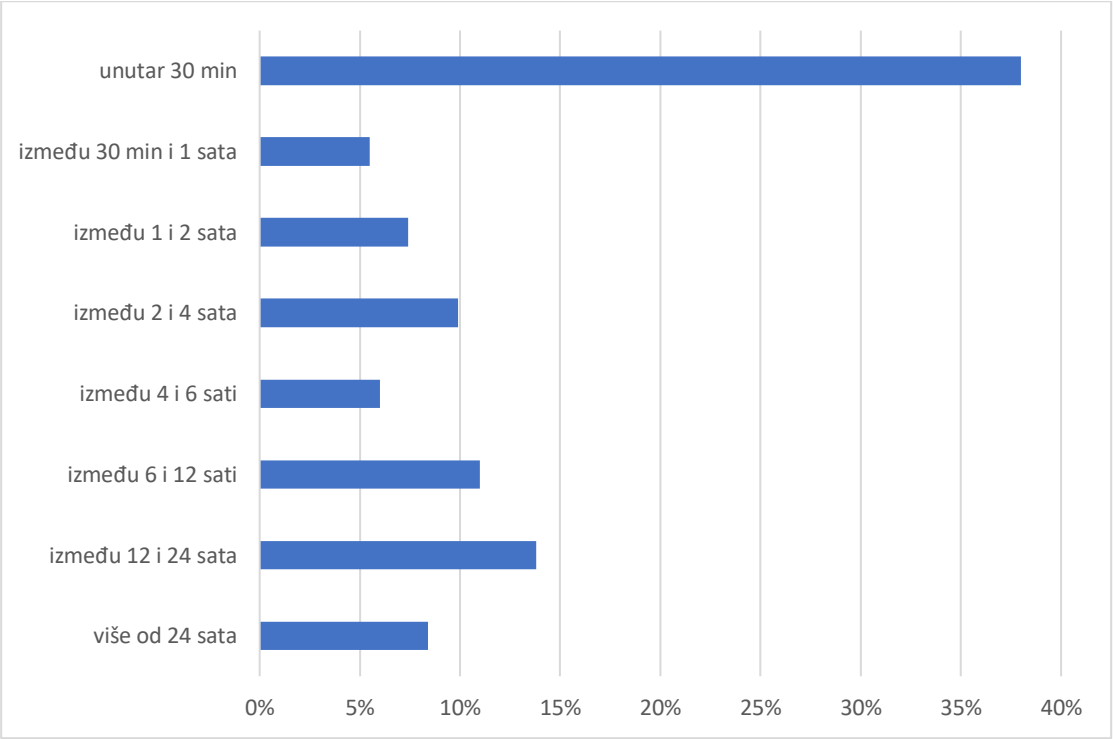


Izvor: izrada autora prema SWIFT, 2022.

Osim platnih transakcija, SWIFT prenosi i poruke o vrijednosnicama, volumen kojih je u periodu od 2016. do 2021. imao prosječni godišnji rast od 11%, za 2,9% viši od platnih transakcija, u apsolutnom iznosu jednak 5,27 milijardi (Swift, 2022). Uz razvijanje SWIFT-ove Globalne inovacije plaćanja (engl. *Global Payments Innovation – GPI*), koja se fokusira na dodatna poboljšanja (Barbey et al., 2017) u transparentnosti i brzini provođenja transakcija, uz manje troškove međunarodnih plaćanja, postavljaju se temelji za daljnji rast.

Korištenjem Swift-gpi sustava prekograničnih plaćanja, 92% internacionalnih plaćanja izvršava se u roku od 24 sata, dok njih 38% stiže krajnje odredište unutar 30 minuta, prikazano na grafu 9. Dodatno, Swift tvrdi da je za transakcije između određenih tržišta, između kojih su minimizirane valutne kontrole, brzina provođenja još brža. Naime, 72% gpi plaćanja iz Ujedinjenog Kraljevstva u Sjedinjene Države stiže u roku od 30 minuta, a 95% stiže u roku od 6 sati, što je usporedivo s domaćim sustavima plaćanja u mnogim zemljama.

Graf 9 Brzina provedbe internacionalne transakcije kroz sustav Swift-gpi



Izvor: izrada autora prema Swift, 2020.

Nadalje, trenutno se na uzorku od trideset banaka testira sustav koji će biti u mogućnosti usklađivati račune korisnika u stvarnom vremenu. No, valja naglasiti da iako obujam internacionalnih plaćanja na svjetskoj razini raste, u određenim dijelovima opada. Kako propisi protiv pranja novca postaju stroži, banke trebaju više povjerenja u korespondentne banke s kojima obavljaju međunarodna plaćanja. Greška od strane korespondentske banke potencijalno može dovesti do velikih kazni, zbog čega se 75% svjetskih banaka povuklo iz određenih korespondentskih bankarskih odnosa između 2011. i 2016. godine. Najviše su zahvaćene visokorizične regije s niskim prometom, kao što su Karibi, Afrika i Polinezija, koje već prijavljuju pad volumena međunarodnih transfera (Barbey et al., 2017).

4. MODEL RANE DETEKCIJE SUMNJIVIH BANKOVNIH TRANSAKCIJA

4.1. Opis podataka

Podaci o transakcijama u modernom kontekstu pohranjuju se u baze podataka. Rastom popularnosti bankovnih aplikacija, nalaže se potreba za korištenjem učinkovitih i sigurnih sustava modeliranja transakcija. Povijesni podaci trebaju sadržavati sve korisnikove transakcije i pružati detaljan prikaz njegove aktivnosti. Dobro modeliranje transakcijskih podataka omogućava analizu povijesnih podataka i olakšava izradu izvješća (Kullaya i Sarojamma, 2020). Polazna je točka definiranje stupaca tablica u bazi podataka te spremanje informacija o transakciji (Musoko, 2020).

Stupci promatranog skupa podataka su:

- jedinstveni identifikator transakcije
- jedinstveni identifikator korisničkog računa
- vrijeme kada se transakcija dogodila
- tip transakcije
- iznos transakcije
- stanje korisničkog računa nakon izvršene transakcije
- država drugog korisnika, u slučaju internacionalne transakcije (izrada autora prema Musoko, 2020)

Radi pojednostavljenog spremanja podataka, kao tipovi transakcija identificirani su gotovinska uplata i isplata s računa, transfer s jednog korisničkog računa na drugi lokalni račun (unutar države) i obrnuto te internacionalni transferi sredstava (ECB, 2022).

Tablica 1 Transakcije jednog od korisničkih računa

id transakcije	korisnikov id	tip transakcije	datum	iznos	saldo nakon transakcije	država drugog korisnika
433	16	lokalni transfer na drugi račun	24.01.2021	51.786	153	x
434	16	gotovinska isplata	25.01.2021	516	-363	x
435	16	gotovinska uplata	29.01.2021	258	-105	x
436	16	lokalni transfer sa drugog računa	02.02.2021	8.474	8.369	x
437	16	gotovinska isplata	09.02.2021	15	8.354	x
438	16	gotovinska isplata	10.02.2021	32	8.322	x
439	16	internacionalni transfer sa drugog rač.	13.02.2021	1.895	10.217	Sierra Leone
440	16	lokalni transfer sa drugog računa	18.02.2021	14	10.231	x
441	16	gotovinska isplata	21.02.2021	188	10.043	x
442	16	internacionalni transfer na drugi rač.	21.02.2021	526	9.517	Senegal
443	16	lokalni transfer sa drugog računa	24.02.2021	279	9.796	x

444	16	gotovinska isplata	01.03.2021	178	9.618	x
445	16	lokalni transfer na drugi račun	03.03.2021	93	9.525	x
446	16	lokalni transfer na drugi račun	08.03.2021	274	9.251	x
447	16	gotovinska isplata	11.03.2021	178	9.073	x
448	16	gotovinska uplata	13.03.2021	135	9.208	x
449	16	gotovinska uplata	17.03.2021	961	10.169	x
450	16	gotovinska uplata	18.03.2021	264	10.433	x
451	16	gotovinska uplata	21.03.2021	269	10.702	x
452	16	gotovinska isplata	22.03.2021	8	10.694	x
453	16	lokalni transfer na drugi račun	28.03.2021	252	10.442	x
454	16	gotovinska isplata	29.03.2021	146	10.296	x
455	16	gotovinska isplata	29.03.2021	90	10.206	x
456	16	lokalni transfer sa drugog računa	03.04.2021	157	10.363	x
457	16	lokalni transfer na drugi račun	09.04.2021	1.405	8.958	x
458	16	lokalni transfer na drugi račun	15.04.2021	15	8.943	x
459	16	lokalni transfer sa drugog računa	20.04.2021	922	9.865	x
460	16	gotovinska uplata	21.04.2021	212	10.077	x

Izvor: izrada autora

Tablica 1. prikazuje transakcije koje pripadaju korisničkom računu 16 (za pregled ukupnog skupa podataka od tristo korisničkih računa i pripadnih 10.000 transakcija korištenih u radu pogledati prilog 2). Transakcije u tablici poredane su kronološki. Prva zabilježena transakcija sa jedinstvenim identifikatorom 433 bila je lokalni transfer sredstava sa gledanog korisničkog računa na drugi, iznosom 51.786€, dok je iznos koji je ostao na računu korisnika, odnosno saldo računa nakon transakcije 153€. Iz navedenog možemo zaključiti da je na računu prije provedbe transakcije bilo 51.939€. Stupac „država drugog korisnika“ označen je sa „x“ pošto nije riječ o transferu van granica države. Promatran korisnički račun 16 bio je predmetom 28 transakcija, prosječne vrijednosti 2.384€, sume 69.542€ u periodu od 24.1.2021. do 21.4.2021. godine. Riječ je o devet isplata i šest uplata gotovine, jedanaest lokalnih transfera sredstava na neki drugi račun ili sa nekog drugog računa te dva internacionalna transfera sredstava, u afričke države Senegal i Sierra Leone. Konačno, dva puta zabilježen je i minus na računu, odnosno negativan saldo.

4.2. Metodologija istraživanja

Financijske institucije moraju se pridržavati propisa koji reguliraju pranja novca. Ključni dio ispunjavanja ovih smjernica je praćenje i blokiranje sumnjivih transakcija, što je je skup proces koji zahtijeva mnogo resursa, sklon je greškama i pokretanju lažno pozitivnih rezultata (Fong, 2022). Proces olakšavaju programska rješenja za praćenje transakcija, koja se rade na temelju

unaprijed definiranih modela, odnosno pravila. Programi za praćenje transakcija omogućuju institucijama izbjegavanje plaćanja kazni, povećanje ugleda i reduciranje operativnih troškova kroz smanjivanje broja ručnih pregleda računa klijenata. Automatski uočavaju sumnjive transakcije, poput velikih gotovinskih depozita i neuobičajene aktivnosti na računu, što stvara ravnotežu između sigurnosti i jednostavnosti korištenja. Korisnicima s niskim rizikom moguće je dopustiti izvršavanje većeg broja radnji (Fong, 2022), dok je fokus na korisnicima sa srednjim i visokim rizikom.

Program za praćenje transakcija prati svaki novi zapisani podatak povezan s transakcijom i provodi te podatke kroz sustavno definirana pravila rizika. Sustav tada automatski prepoznaje i označava sumnjive radnje kao što su: (i) neuobičajene transakcije ili aktivnosti na računu, (ii) transakcije iznad određene vrijednosti, (iii) međunarodne transfere iznad određene vrijednosti, (iv) velike gotovinske depozite ili podizanja novca, (v) nepoznate izvore ulaznih i izlaznih sredstava na račun (Fong, 2022).

Za osiguranje dobrog praćenja transakcija potrebno je kombinirati nadzor transakcija i samih korisnika. Naime, poželjno je biti u mogućnosti potvrditi identitete stranaka i ukomponirati te podatke kao dio svoje strategije. Što je potvrda identiteta točnija, jednostavnije je uočiti odstupanja u aktivnostima računa i poboljšati usklađenost na svim razinama. Nadalje, potrebno je uspoređivati aktivnosti korisničkih računa sa referentnom vrijednošću, koja se gradi na temelju ponašanja tipičnog korisnika. Potrebno je pratiti i učestalost transakcija, u smislu prepoznavanja sumnjivih aktivnosti na temelju brzog pomicanja novčanih sredstava koji odstupaju od uobičajenih, uz automatsko izostavljanje ekstremnih vrijednosti i redovitih velikih depozita kao što su plaća i veći honorari pojedinca. Konačno, poželjno je pohranjivati informacije o transakcijama u bazu podataka koja može služiti za retroaktivnu analizu (Fong, 2022).

Skupovi pravila u praćenju pranja novca mogu biti jednostavni ili složeni koliko regulacija i sama institucija zahtijeva. Primjerice, moguće je definirati pravilo koje u slučaju da netko pokuša izvršiti plaćanje na određeni račun blokira transakciju i generira upozorenje. Takav stil restrikcijskih pravila podrazumijeva postojanje crne liste korisnika, zemalja ili drugog čimbenika te ona propuštaju samo transakcije koje nisu u doticaju s crnom listom. Valja naglasiti da su crne liste vremenski skupe, odnosno ubrzano usporavaju rad sustava s porastom broja transakcija. Za ulazak u trag suptilnijim načinima pranja novca, potrebni su skupovi pravila, koji su kompleksniji. Primjer takvog skupa pravila je: ako se više od četiri računa prijavi s iste internetske adrese unutar određenog broja minuta, blokirati adresu na jedan sat i

generirati upozorenje. Skupovi pravila definiraju radnje koje treba poduzeti, uključujući trenutak pošiljanja upozorenja (SEON, 2022).

Sustav može imati stotine pravila koja se međusobno nužno ne isključuju, određena interakcija može ih aktivirati nekoliko, time povećavajući ocjenu rizika transakcije. Kao rezultat toga, sustav može slati upozorenje i tražiti osobnu intervenciju analitičara. Rješenje za praćenje transakcija treba biti fleksibilno, za lakšu prilagodbu potrebama korisnika, skalabilno, da bi se osigurala brza provedba unatoč potencijalnim budućim rastućim potrebama i redovno ažurirano za promjene u zakonu i novootkrivene sheme pranja novca (SEON, 2022).

Identificirana pravila modela rane detekcije sumnjivih bankovnih transakcija određuju da sumnjivim treba označiti:

- transakcije iznad vrijednosti 9.500€ (5% umanjeno od zakonski predviđenog iznosa od 10.000€ radi predostrožnosti)
- međunarodne transfere iznad polovice vrijednosti tuzemne sumnjive transakcije (4.750€)
- neobjašnjene masovne transakcije gotovinom i monetarnim instrumentima u iznosu iznad 9.500€
- velik broj transakcija u kratkom vremenskom razdoblju (>75 u 48 sati), posebno u računima koji obično ne bilježe puno aktivnosti
- izvor ulaznih i izlaznih sredstava na račun je sa poznatog drugog sumnjivog računa
- međunarodne transfere u ili iz visokorizičnih država (na temelju liste visokorizičnih trećih država i poreznih oaza Europske Komisije s niskom učinkovitošću sustava protiv pranja novca, tablica 2.)
- transakcije i/ili obujmi ukupne aktivnosti koji nisu u skladu s očekivanom aktivnošću i svrhom računa identificirane u trenutku otvaranja korisničkog računa
- transakcije identificirane kao neke u lancu složenog niza transakcija koji uključuje više računa, banaka, stranki i jurisdikcija i ukazuje na slojevitu aktivnost
- neregularne transakcije ili aktivnosti na računu (izrada autora prema Financial Crimes Enforcement Network, 2003, HANFA, 2015, Fong, 2022)

Tablica 2 Države s visokim rizikom za pranje novca

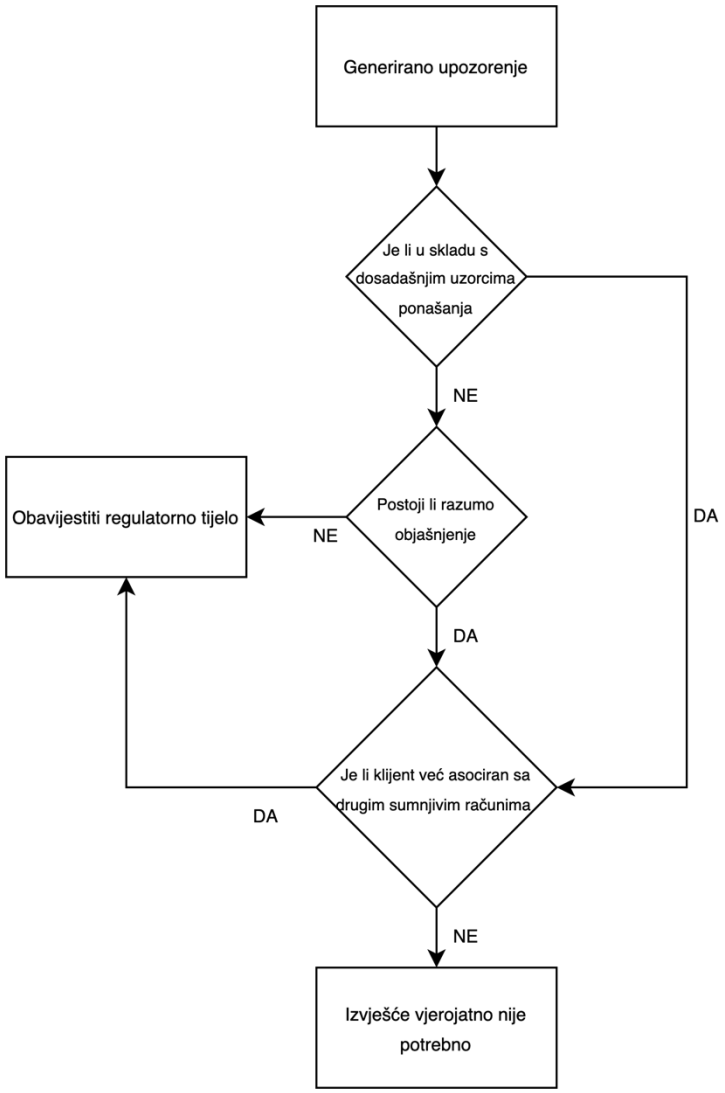
	Datum stupanja na snagu
Afganistan	23.09.2016
Barbados	01.10.2020
Burkina Faso	13.03.2022

Kambodža	01.10.2020
Kajmanski otoci	13.03.2022
Demokratska narodna Republika Koreja	23.09.2016
Haiti	13.03.2022
Iran	23.09.2016
Jamajka	01.10.2020
Jordan	13.03.2022
Mali	13.03.2022
Maroko	13.03.2022
Mijanmar	01.10.2020
Nikaragva	01.10.2020
Pakistan	22.10.2018
Panama	01.10.2020
Filipini	13.03.2022
Senegal	13.03.2022
Južni Sudan	13.03.2022
Sirija	23.09.2016
Trinidad i Tobago	06.03.2018
Uganda	23.09.2016
Vanuatu	23.09.2016
Jemen	23.09.2016
Zimbabve	01.10.2020

Izvor: izrada autora prema Europska Komisija, 2022.

Podaci označenih transakcija obično se akumuliraju u posebnoj datoteci koja se zove izvješće o sumnjivim aktivnostima (engl. *Suspicious Activity Report - SAR*), koje je formatirano na poseban način kako bi ga financijski analitičari i regulatori mogli pregledati u standardiziranom obliku (Fong, 2022). Općenito, izvješće o sumnjivim transakcijama trebalo bi identificirati par bitnih elemenata: tko, što, kada, gdje, zašto i kako. Konkretno, treba identificirati tko provodi sumnjivu aktivnost, koji se instrumenti i mehanizmi koriste za provođenje sumnjive transakcije, kada i gdje se sumnjiva transakcija dogodila, je li se dogodila u stranoj jurisdikciji, zašto je sumnjiva i, konačno, kako se dogodila, i to na koncizan, točan i logičan način. (Financial Crimes Enforcement Network, 2003). Izlazi programa za praćenje transakcija trebaju olakšavati popunjavanje izvješća o sumnjivim aktivnostima.

Slika 1 Dijagram odluke treba li institucija obavijestiti regulatorno tijelo o sumnjivoj transakciji



Izvor: izrada autora prema Fong, 2022.

Dijagram na slici 1. prikazuje tijek odluke u modelu treba li transakciju koja je generirala upozorenje prijaviti regulatornom tijelu kao sumnjivu. Podrazumijeva osobni angažman zaposlenika koji donosi odluku na temelju informacija koje mu pruža sustav te povijesti korisničkog računa koji je u pitanju. Prvo se provjerava odskače li transakcija od dosad zabilježenih uzoraka ponašanja korisnika, ako ne, postoji li razumno objašnjenje za odskakanje te u slučaju da je odgovor na oba pitanja ne, valja podnijeti prijavu. Alternativno, u slučaju da objašnjenje postoji, a klijent je u prošlosti već imao kontakt sa drugim računima koji su bilježili sumnjivu aktivnost, također se preporuča podnošenje prijave.

4.3. Rezultati istraživanja

Primjenom modela detekcije sumnjivih bankovnih transakcija na transakcijama korisničkog računa 16, prije sagledanog u sklopu tablice 1., podaci se proširuju za stupce koji redom ispisuju radi li se o visokorizičnoj državi, je li transakcija izvršena sa ili na već poznati drugi sumnjivi račun, kratak opis razloga za sumnju te, konačno, procjene smatra li se transakcija sumnjivom na temelju zadanih pravila modela.

U tablici 3. moguće je vidjeti da su modelom rane detekcije dvije od ukupno 28 transakcija korisnika 16 prepoznate kao sumnjive. Prva sumnjiva transakcija, sa jedinstvenim identifikatorom 433, je transfer sredstava na drugi račun unutar države u iznosu od 51.786 € te ju model označava sumnjivom na temelju prvog pravila (iznos transakcije je iznad 9.500 €). Druga sumnjiva transakcija s identifikatorom 442 bilježi internacionalni prijenos sredstava u Senegal, visokorizičnu državu prema šestom pravilu, odnosno tablici 2., što ju u modelu automatski čini sumnjivom neovisno o količini transferiranih sredstava, u ovom slučaju 526 €. Niti jedna transakcija na izdvojenom korisničkom računu 16 nije transferirana sa ili na već od prije poznat sumnjivi račun.

Tablica 3 Transakcije korisničkog računa 16 proširene za stupce modela

id transakcije	korisnikov id	tip transakcije	datum	iznos	saldo nakon transakcije	država drugog korisnika	visokorizična država	transferirano sa/na sumnjiv račun	razlog za sumnju	sumnjiva
433	16	lokalni transfer na drugi račun	24.01.2021	51.786	153	x	NE	NE	iznos > 9.500€	DA
434	16	gotovinska isplata	25.01.2021	516	-363	x	NE	NE	x	NE
435	16	gotovinska uplata	29.01.2021	258	-105	x	NE	NE	x	NE
436	16	lokalni transfer sa drugog računa	02.02.2021	8.474	8.369	x	NE	NE	x	NE
437	16	gotovinska isplata	09.02.2021	15	8.354	x	NE	NE	x	NE
438	16	gotovinska isplata	10.02.2021	32	8.322	x	NE	NE	x	NE
439	16	internacionalni transfer sa drugog rač.	13.02.2021	1.895	10.217	Sierra Leone	NE	NE	x	NE
440	16	lokalni transfer sa drugog računa	18.02.2021	14	10.231	x	NE	NE	x	NE
441	16	gotovinska isplata	21.02.2021	188	10.043	x	NE	NE	x	NE
442	16	internacionalni transfer na drugi rač.	21.02.2021	526	9.517	Senegal	DA	NE	visokorizična zemlja	DA
443	16	lokalni transfer sa drugog računa	24.02.2021	279	9.796	x	NE	NE	x	NE
444	16	gotovinska isplata	01.03.2021	178	9.618	x	NE	NE	x	NE
445	16	lokalni transfer na drugi račun	03.03.2021	93	9.525	x	NE	NE	x	NE
446	16	lokalni transfer na drugi račun	08.03.2021	274	9.251	x	NE	NE	x	NE
447	16	gotovinska isplata	11.03.2021	178	9.073	x	NE	NE	x	NE

448	16	gotovinska uplata	13.03.2021	135	9.208	x	NE	NE	x	NE
449	16	gotovinska uplata	17.03.2021	961	10.169	x	NE	NE	x	NE
450	16	gotovinska uplata	18.03.2021	264	10.433	x	NE	NE	x	NE
451	16	gotovinska uplata	21.03.2021	269	10.702	x	NE	NE	x	NE
452	16	gotovinska isplata	22.03.2021	8	10.694	x	NE	NE	x	NE
453	16	lokalni transfer na drugi račun	28.03.2021	252	10.442	x	NE	NE	x	NE
454	16	gotovinska isplata	29.03.2021	146	10.296	x	NE	NE	x	NE
455	16	gotovinska isplata	29.03.2021	90	10.206	x	NE	NE	x	NE
456	16	lokalni transfer sa drugog računa	03.04.2021	157	10.363	x	NE	NE	x	NE
457	16	lokalni transfer na drugi račun	09.04.2021	1.405	8.958	x	NE	NE	x	NE
458	16	lokalni transfer na drugi račun	15.04.2021	15	8.943	x	NE	NE	x	NE
459	16	lokalni transfer sa drugog računa	20.04.2021	922	9.865	x	NE	NE	x	NE
460	16	gotovinska uplata	21.04.2021	212	10.077	x	NE	NE	x	NE

Izvor: izrada autora

Model je za svih tristo promatranih korisničkih računa i pripadajućih 10.000 transakcija sumnjivima označio njih 119, što predstavlja 1,19% ukupnog uzorka podataka. Suma svih sumnjivih transakcija je 1.399.790€. Najčešći razlog za sumnju je transakcija na drugi, ili sa drugog računa registriranog u banci u visokorizičnoj zemlji, njih 56%, uključujući porezne oaze Kajmanske otoke i Panamu, analizirane u sklopu poglavlja 2.4. i grafa 1. Dodatno, zabilježeno je 44 transakcija u vrijednosti iznad 9.500€, te osam internacionalnih transakcija u vrijednosti iznad 4.750€. Nisu zabilježeni slučajevi velikog broja transakcija u kratkom vremenskom razdoblju, odnosno više od 75 transakcija na istom računu unutar 48 sati, kao ni slučajeva transfera sredstava na račun od prije poznatog drugog sumnjivog računa i obrnuto. Konačno, zabilježeno je 19 korisničkih računa sa dvije sumnjive transakcije, dok računi 159, i 204 imaju po tri. Tablica 4. prikazuje sumnjive transakcije prvih pedeset korisničkih računa.

Tablica 4 Sumnjive transakcije detektirane modelom rane detekcije za prvih 50 korisničkih računa

id transakcije	korisnikov id	tip transakcije	datum	iznos	saldo nakon transakcije	država drugog korisnika	visokorizična država	transferirano sa/na sumnjiv račun	razlog za sumnju	sumnjiva
81	3	internacionalni transfer na drugi rač.	02.04.2021	281	57.669	Filipini	DA	NE	visokorizična zemlja	DA
94	3	internacionalni transfer na drugi rač.	11.05.2021	85	47.018	Afganistan	DA	NE	visokorizična zemlja	DA
117	4	internacionalni transfer sa drugog rač.	18.04.2021	101	63.253	Haiti	DA	NE	visokorizična zemlja	DA
179	7	internacionalni transfer sa drugog rač.	28.01.2021	6	56.472	Iran	DA	NE	visokorizična zemlja	DA
231	8	internacionalni transfer sa drugog rač.	07.04.2021	96	53.340	Trinidad i Tobago	DA	NE	visokorizična zemlja	DA
236	9	internacionalni transfer na drugi rač.	22.01.2021	23	58.463	Senegal	DA	NE	visokorizična zemlja	DA

339	12	gotovinska uplata	03.04.2021	9.767	38.550	x	NE	NE	iznos > 9.500€	DA
433	16	lokalni transfer na drugi račun	24.01.2021	51.786	153	x	NE	NE	iznos > 9.500€	DA
442	16	internacionalni transfer na drugi rač.	21.02.2021	526	9.517	Senegal	DA	NE	visokorizična zemlja	DA
602	21	internacionalni transfer sa drugog rač.	17.03.2021	8.697	42.954	Latvija	NE	NE	internac. transakcija > 4750€	DA
617	21	internacionalni transfer sa drugog rač.	27.04.2021	12	45.836	Panama	DA	NE	visokorizična zemlja	DA
628	22	internacionalni transfer na drugi rač.	03.03.2021	68	67.260	Nikaragva	DA	NE	visokorizična zemlja	DA
629	22	internacionalni transfer sa drugog rač.	09.03.2021	109	67.369	Nikaragva	DA	NE	visokorizična zemlja	DA
808	28	gotovinska uplata	16.05.2021	9.655	78.732	x	NE	NE	iznos > 9.500€	DA
814	29	internacionalni transfer na drugi rač.	21.01.2021	4.924	41.743	Antarktika	NE	NE	internac. transakcija > 4750€	DA
848	30	internacionalni transfer na drugi rač.	11.02.2021	177	45.564	Kajmanski otoci	DA	NE	visokorizična zemlja	DA
849	30	internacionalni transfer na drugi rač.	13.02.2021	107	45.457	Iran	DA	NE	visokorizična zemlja	DA
893	32	lokalni transfer na drugi račun	04.02.2021	9.520	22.689	x	NE	NE	iznos > 9.500€	DA
944	33	internacionalni transfer na drugi rač.	25.04.2021	52	54.671	Trinidad i Tobago	DA	NE	visokorizična zemlja	DA
955	34	internacionalni transfer na drugi rač.	25.01.2021	1.395	57.128	Albanija	DA	NE	visokorizična zemlja	DA
1273	43	internacionalni transfer na drugi rač.	21.02.2021	172	35.404	Maroko	DA	NE	visokorizična zemlja	DA
1289	43	internacionalni transfer sa drugog rač.	18.04.2021	1.504	42.303	Jordan	DA	NE	visokorizična zemlja	DA
1317	45	internacionalni transfer sa drugog rač.	05.02.2021	292	83.672	Jordan	DA	NE	visokorizična zemlja	DA
1349	46	lokalni transfer na drugi račun	23.01.2021	31.139	21.031	x	NE	NE	iznos > 9.500€	DA
1380	47	internacionalni transfer sa drugog rač.	26.01.2021	4.831	61.483	Malta	NE	NE	internac. transakcija > 4750€	DA
1416	48	gotovinska uplata	09.02.2021	9.746	52.836	x	NE	NE	iznos > 9.500€	DA
1481	50	internacionalni transfer sa drugog rač.	24.02.2021	134	23.826	Mijanmar (Burma)	DA	NE	visokorizična zemlja	DA

Izvor: izrada autora

4.4. Ograničenja istraživanja

U okolnostima zabranjene distribucije stvarnih podataka o bankovnim transakcijama pojedinaca, radi Opće uredbe o zaštiti podataka 2016/679/EZ u Europskoj uniji (Eur-Lex, 2016.), ili sličnih zakona o tajnosti podataka na drugim prostorima, podaci korišteni u radu generirani su računalnim programom (postupak je ukratko opisan u prilogu 1.). Predstavljaju pojednostavljenu sliku realnosti i stvoreni su s namjerom prezentiranja načina na koji funkcionira model detekcije sumnjivih transakcija iznesen u radu, kao i njegovog testiranja.

Nadalje, prepoznaje se nedostatak povijesnih podataka banke na temelju kojih je moguće napraviti profil korisnika i njegovih obrazaca ponašanja u vidu potrošačkih navika, izvora prihoda i slično, na temelju kojih bi bilo moguće utvrditi odstupanja od uobičajenog, što bi

modelu dalo novu dimenziju preciznosti prepoznavanja sumnjivih transakcija. Povijesni, odnosno stariji podaci korisničkih računa potencijalno su mogli biti generirani istim računalnim programom kojim su stvorene i transakcije analizirane u radu, no od te se ideje odustalo pošto oni ne bi predstavljali obrasce ponašanja stvarne osobe, već bi se ulazilo u analizu funkcioniranja samog programa za stvaranje transakcija.

4.5. Unaprjeđenje modela korištenjem modernih tehnologija

4.5.1. Veliki podaci i rudarenje podataka u kontekstu detekcije pranja novca

Ograničenje tradicionalnog pristupa praćenja isključivo transakcija u svrhu detekcije pranja novca je nedovoljna preciznost. Analize pokazuju da je do 90 % svih upozorenja koja generiraju takvi sustavi lažno pozitivna. Stvaraju se veliki operativni troškovi, a i demotivirajući uvjeti za analitičare koji ih proučavaju (Demetis, 2018), što potencijalno smanjuje njihov učinak u situacijama opravdanog i stvarnog razloga za sumnju. Danas je proces detektiranja pranja novca znatno kompleksniji uporabom novih tehnologija.

Razvitak tehnologije stvorio je uvjete generiranja i učinkovitog pohranjivanja informacija, što u kontekstu velikog broja korisnika rezultira enormnim rastom količine podataka i informacija koje poduzeća prikupljaju na dnevnoj bazi. Posljedično, otvara se prilika za njihovom analizom i korištenjem (Dong i Tjortjis, 2003). Podaci filtrirani iz različitih izvora skupljaju se u jedinstvenu integriranu bazu podataka zvanom skladište podataka (engl. *data-warehouse*) (Watkins et al., 2003) koja služi za daljnju analizu i kreaciju izvješća.

Pojam velikih podataka (engl. *Big-Data*), odnosi se na stalno rastuću količinu strukturiranih i nestrukturiranih informacija različitih formata, koje pripadaju istom kontekstu. Koriste se za rješavanje nestandardnih poslovnih izazova, skupljaju se iz različitih izvora podataka i obično su preveliki da bi ih analizirali klasični sustavi obrade informacija (Ostapchenya, 2021), zbog čega potiču razvijanje tehnoloških sustava koji su u stanju obraditi ih. Osnovni izazov velikih podataka je na koji ih način istražiti i iz njih izvući korisne informacije i znanje, što podrazumijeva osiguravanje financija, ljudi, i potrebne infrastrukture za projekt. Nadalje, zahtijevaju pažljivo upravljanje podacima, uključujući njihove izvore, kvalitetu i sadržaj, kao i ograničavanje pristupa samo na obučene pojedince kako bi se osigurala sigurnost, dosljednost i točnost podataka.

Glavna svojstva velikih podataka su:

- velik volumen generiranih i prikupljenih podataka
- brzina kojom se stvaraju/generiraju, a u konačnici i obrađuju i analiziraju

- njihova raznolikost (strukturirani, polustrukturirani i nestrukturirani podaci)
- istinitost
- varijabilnost (Chedrawi, Atallah i Osta, 2020).

Banke imaju koristi od velikih podataka jer mogu brzo i jednostavno izvući relevantne informacije iz podataka koje već imaju i pretvoriti ih u značajne koristi za sebe i svoje klijente. Informacije sadržane u tim podacima mogu biti iznimno vrijedne u smislu omogućavanja boljeg upravljanja rizikom, regulatornom usklađenošću i otkrivanjem financijskog kriminala, razumijevanja ponašanja i potreba korisnika te kretanja novca (Srivastava i Gopalkrishnan, 2015.). Dodatno, korisne su za analizu klijentovog prihoda i potrošnje, segmentaciju potrošača i upravljanje povratnim informacijama. Naime, kad ljudi daju povratne informacije o radu financijske institucije telefonom ili na internet stranici, ostavljaju komentare i iznose svoje mišljenje na društvenim mrežama i drugim internetskim stranicama (Ostapchenya, 2021) dostupnim široj javnosti, indirektno omogućavaju analizu tih (velikih) podataka.

Kroz korelaciju višedimenzionalnih informacija, moguće je profilirati svakog pojedinca na temelju velikih podataka i doći do zaključaka o njegovoj kreditnoj sposobnosti, sklonostima i tendencijama, obrascima ponašanja, preferencijama, navikama i drugim karakteristikama (Chedrawi, Atallah i Osta, 2020), obično s obrazloženjem da mu se želi pružiti kvalitetnija i preciznija usluga.

U kontekstu modela rane detekcije sumnjivih transakcija, rezultati takve analize mogu se koristiti za donošenje konačne odluke je li određen korisnički račun sumnjiv ili nije, moralnost čega nije predmet ovog istraživanja.

Među podacima je moguće uočiti ponavljajuće uzorke, povezanosti i kauzalnosti te ih dokumentirati, što je stvorilo polje istraživanja zvano otkrivanje znanja u bazama podataka (engl. *Knowledge Discovery in Databases*), ili rudarenje podataka (engl. *data-mining*) (Scott et al., 1998). Otkrivanje znanja u bazama podataka je kompleksan proces identificiranja valjanih, novih, korisnih i u konačnici razumljivih obrazaca u podacima.

Kombiniraju se tehnike iz područja baza podataka, statistike i vizualizacije, u novije vrijeme i umjetne inteligencije. Sam proces ima više faza i iterativan je. Podrazumijeva sljedeće korake: (i) definiranje cilja procesa, primjerice, izgradnju opisnog modela kupca koji će predviđati njegovo ponašanje prema nekom apstraktnom mjerilu, (ii) selekciju i filtraciju skupa podataka na temelju relevantnosti, (iii) pripremu podataka, (iv) odabir algoritma za rudarenje podataka, (v) samo rudarenje, odnosno traženje informacija i uzoraka, (vi) tumačenje rezultata te,

konačno, (vii) konsolidiranje znanja, odnosno upotreba dobivenog znanja na koristan način (Scott et al., 1998).

Peti korak, rudarenje podataka, je računski najkompleksniji i izvediv na više načina. Osnovna tehnika je asocijacija, koja se često koristi za najveće skupove podataka. To je tehnika pronalaženja obrazaca u smislu povezanosti jednog događaja s drugim (Bhambri, 2011). Nastoje se otkriti povezanosti među atributima u bazama podataka, proizvodeći ako-onda (engl. *if-then*) izjave o vrijednostima atributa. Primjerice, ako se neki atributi X i Y dovedu u vezu, u bazi podataka gdje se u transakcijama pojavljuje X, postoji vjerojatnost da će se pojaviti i Y. Snaga takve veze izražava se u postotku. Valja naglasiti da algoritmi za rudarenje podataka na temelju asocijacija obično pronađu puno pravila od kojih nisu sva relevantna (Garcia et al., 2008), zbog čega ih je potrebno filtrirati na temelju prethodno definiranih pragova ili subjektivne procjene relevantnosti.

Slijedeća relevantna tehnika je klasifikacija, koja je ujedno i najkorištenija u praksi. Ona na temelju unaprijed definiranih karakteristika i pravila klasificira podatke skupa. Često uključuje algoritme klasifikacije temeljene na neuronskim mrežama (koje će biti analizirane u nastavku) i stabla odluke, što ovu tehniku čini pogodnom za detektiranje financijskih prijevara i pranja novca. Cilj je razviti točna predviđanja unutar svake pojedine klase. Postavljena pravila klasifikacije testiraju se na starim, povijesnim skupovima podataka te se u slučaju prihvatljive razine točnosti primjenjuju na aktualne podatke (Garcia et al., 2008).

Model rane detekcije sumnjivih bankovnih transakcija prezentiran u sklopu poglavlja 4.2. koristi određene karakteristike klasifikacije, dok bi uporabom tehnike asocijacije u teoriji postao još precizniji.

Trenutno najkorištenija programska rješenja za rudarenje podataka su:

- Orange Data Mining, koji je napisan u programskom jeziku Python i razvijen u Sloveniji, u sklopu Sveučilišta u Ljubljani. Temeljen je na komponentama (takozvanim *widgetima*), besplatan za korištenje i omogućuje prikaz podataka u obliku tablica, njihovo filtriranje, formatiranje, transferiranje i, konačno, rudarenje i vizualizaciju
- SAS Data Mining (Sustav Statističke analize, Statistical Analysis System), kojeg je razvio SAS Institut i može rudariti podatke, mijenjati ih, upravljati i analizirati statističkim metodama. Nudi grafičko korisničko sučelje što ga čini pogodnim za neprofesionalne korisnike.
- DataMelt Data Mining, napisan u programskom jeziku Javi i prvenstveno namijenjen studentima i inženjerima

- Rattle, koji proširuje programski jezik za statistički prikaz i obradu podataka R sa funkcionalnostima rudarenja podataka
- Rapid Miner, koji je napisan u Javi i koristi se za predviđanja na temelju trendova (Javapoint, 2021a).

Korištenjem tehnika rudarenja podataka, razvijeni su kompleksniji pristupi profiliranja osobe temeljeni na rizičnosti (Demetis, 2018) i kalkulirani na temelju povijesnih podataka podnijetih izvještaja o sumnjivim aktivnostima i transakcijama, koji su primjenjivani na svakom pojedinom klijentu.

Tablica 5 Ponderi rizičnosti za pranje novca po karakteristikama (0 - nisko, 5 - visoko)

Karakteristika	Ponder
Spol	muškarci (1.52), žene (0.62)
Dobna skupina	< 18 (1.04), 18-24 (1.66), 25-34 (1.71), 35-44 (1.45), 45-54 (1.04), 55-64 (0.71), 65+ (0.33)
Bračni status	samac (1.90), drugo (0.92)
Visokorizične skupine poštanskih brojeva	npr. Merchant City - G1 (2.82), Blythswood Hill - G2 (1.3), Anderston, Yorkhill… - G3 (0.83) itd.
Imigrant	da (2.7), ne (1.0)
Vlasnik/ca tvrtke	vlasnik (1.92), nije-vlasnik (0.95)

Izvor: izrada autora prema Demetis, 2018.

Banka u Ujedinjenom Kraljevstvu promatrana u sklopu istraživanja Demetisa razvila je sustav koji je pripisivao rizičnosti pojedinca na temelju relevantnih karakteristika kao što su spol, dob, bračni status, lokacija, državljanstvo te vlasništvo tvrtke. Karakteristikama su dodjeljivani ponderi rađeni na temelju specifičnosti kao što su pojedinčeva imovina, prihod, saldo računa, ukupno zaduženje, vrijeme izvršenja transakcija, njihov broj i vrsta, iznosi prekoračenja, omjer kartičnog i gotovinskog plaćanja, količinu međunarodnih transakcija osoba o kojima su prije podnijeti izvještaji o sumnjivoj aktivnosti (SAR izvještaji) i slično (za naveden sustav nisu korištene sve moderne prednosti velikih podataka, već samo interni podaci banke).

Puni rezultati analiza i odgovarajući ponderi dani su u tablici 5, a najrizičnijim opisuju muškarca imigranta, koji nije u vezi, dobi 25 do 34 godine, živi na lokaciji Merchant City, Glasgow (poštanski broj G1) i sam je vlasnik tvrtke.

4.5.2. Aplikacije umjetne inteligencije i strojnog učenja

Umjetna inteligencija grana je računalne znanosti koja nastoji stvoriti inteligentne strojeve i programe koji se ponašaju kao ljudi, razmišljaju kao ljudi i imaju sposobnost donošenja vlastitih odluka, učenja, prosuđivanja i rješavanja problema. Omogućava izgradnju programa i uređaja koji su sposobni jednostavno i precizno riješiti probleme iz stvarnog svijeta. Aktualno se koristi u poljima samovozećih automobila, igranja šaha, dokazivanja matematičkih teorema, sviranju glazbe, slikanju, planiranju kirurških zahvata, rješavanju logističkih problema u prometu, marketingu, financijama itd. Pruža mogućnost kreiranja osobnih virtualnih pomoćnika, kao što su Cortana, Google asistent i Siri (Javapoint, 2021b).

Ciljevi umjetne inteligencije su:

- repliciranje ljudske inteligencije
- rješavanje zadataka koji zahtijevaju veliko znanje
- pronalazak inteligentne veze između percepcije i djelovanja
- izgradnja stroja koji može obavljati zadatke koji zahtijevaju ljudsku inteligenciju
- razvijanje sustava koji pokazuje značajke inteligentnog ponašanja, učenja novih stvari, uz mogućnost pružanja demonstracija, objašnjenja i savjetovanja korisnika

Umjetnu inteligenciju odlikuje velika brzina donošenja odluka, visoka preciznost, pouzdanost i mali broj grešaka, može izvršiti istu radnju n puta s konstantnom točnošću i pogodna je za korištenje u područjima rizičnima za ljude (situacije kao što su deaktiviranje bombe, istraživanje dna oceana itd.). S druge strane, prepoznati nedostaci umjetne inteligencije su visoka cijena razvijanja i održavanja, nije u mogućnosti razmišljati van zadanih okvira unutar kojih je programirana, nije kreativna niti emotivna te povećava ljudsku ovisnost o strojevima (Javapoint, 2021b).

Strojno učenje (engl. *Machine learning – ML*) potpodručje je umjetne inteligencije koje omogućuje strojevima da uče iz prošlih, povijesnih podataka i iskustava. Koristi velike količine strukturiranih i polustrukturiranih podataka kako bi iz njih izradilo kompleksne modele koji daju predviđanja, a prema mogućnosti i konkretne rezultate. Cilj strojnog učenja je omogućiti strojevima/programima da uče iz podataka kako bi mogli dati točan rezultat. Uglavnom se bavi uočavanjem obrazaca i može obavljati samo specifične poslove za koje je osposobljeno. Ima mogućnost poboljšavanja i samo ispravljanja kad mu se preda nova i veća količina podataka (Javapoint, 2021c).

Neke od najpopularnijih tehnika koje strojno učenje može koristiti u otkrivanju i suzbijanju aktivnosti pranja novca prikazane su u tablici 6.

Tablica 6 Tehnike koje strojno učenje koristi za otkrivanje i suzbijanje aktivnosti pranja novca

Tehnika	Opis
Logistička regresija	Uključuje kategoričke varijable kao što su "da/ne" ili "muško/žensko". Često korišteno.
Indukcijski algoritmi	Algoritmi koji generiraju stabla odlučivanja na temelju povijesnih rezultata.
Neuronske mreže	Tehnika umjetne inteligencije koja oponaša ljudski mozak učenjem i pohranjivanjem ulaznih i izlaznih podataka.
Neizrazita (engl. *fuzzy*) logika	Omogućuje obradu nepotpunih informacija na temelju kojih izvodi zaključke.

Izvor: izrada autora prema Watkins et al., 2003.

Logistička regresija može riješiti probleme koje uključuju kategoričke varijable (npr. varijable koje se mogu opisati odgovorom da/ne ili je odgovor na njih muško/žensko). Ova tehnika procjenjuje sve transakcijske zapise i prikazuje ih u brojnim grafičkim formatima prema želji korisnika. Kad su podaci prezentirani na takav način, njihove poveznice postaju jasnije i evidentnije. Korištenjem logističke regresije, grafički prikazi trendova u podacima prikazuju se u višedimenzionalnom formatu pomoću raznih boja i oblika, automatski i bez intervencije radnika. Posljedično, istražitelj pred sebe dobije veliku masu već analiziranih podataka u formatu kojim može upravljati, što uvelike ubrzava i olakšava identifikaciju trendova i uzoraka pranja novca (Watkins et al., 2003).

Indukcijski algoritmi jedna su od tehnika strojnog učenja koja može otkriti obrasce pranja novca. Tehnika klasificira podatke o financijskim transakcijama u kategorije na temelju ponavljajućih uzoraka koje pronalazi u podacima. Ova se metodologija može koristiti za generiranje stabla odlučivanja, a zatim se koristiti za izradu pravila iz povijesnih podataka (Watkins et al., 2003). Stabla odlučivanja omogućuju vizualnu reprezentaciju podataka što ih čini intuitivnijima i lakšim za razumjeti. Spadaju među jednostavnije metode, lakše ih je izračunati, što ih čini vrijednim proučavanja (Hagenlocher, 2017).

Korisnost induktivnih algoritama proizlazi iz njihove sposobnosti da stvore nove poveznice koje osobe obično ne bi uspjele uočiti, time potencijalno otkrivajući korelacije u naizgled nepovezanim transakcijama koje su dio određene kompleksne sheme pranja novca. Tako istražitelju olakšava razumijevanje funkcioniranja određene operacije pranja novca. Dodatno,

pronađene sličnosti i obrasci se naknadno mogu koristiti za poboljšanje i reviziju starih, kao i uspostavljanja novih skupova pravila.

Slijedeća relevantna metodologija koja je korisna u detektiranju pokušaja pranja novca je neuronska mreža. Bazira se na oponašanju procesa učenja ljudskog mozga, od kuda i ime. Neuronska mreža prihvaća nekoliko ulaza, izvodi niz matematičkih operacija nad podacima i proizvodi jedan ili više izlaza. Funkcionalnost nalikuje ljudskom mozgu jer neuronske mreže uče iz danih primjera ulaza i željenih izlaza i pohranjuju to znanje (Watkins et al., 2003).

Neuronska mreža sastoji se od mnoštva pojedinačnih neurona koji primaju i obrađuju signale te ih šalju sljedećim neuronima na daljnju obradu (Faraji, 2022). Više neurona formira sloj, a cijela neuronska mreža ima tri sloja: ulazni sloj, koji prihvaća unose, odnosno varijable, skriveni sloj, koji izvodi sve izračune kako bi pronašao skrivene značajke i uzorke te izlazni sloj, koji prenosi informacije iz skrivenog sloja prema van (Lokanan, 2022, Javapoint, 2021d). Neuronske mreže su korisne kod razvijanja prediktivnih modela i mogu se analizirati pomoću istih metrika performansi kao klasični modeli strojnog učenja. Cijela mreža razvija se i uči na temelju danih podataka te naknadno može s visokom preciznošću detektirati pokušaje pranja novca. Analize pokazuju da je najpreciznija za klasifikaciju rijetkih događaja (Lokanan, 2022).

U praksi se često javljaju slučajevi u kojima su skupovi podataka nepotpuni, ponavljajući i neprecizni, što rezultira neučinkovitim trošenjem resursa i vremena. Neizrazita logika pomaže u smanjenju količine vremena potrebnog za sortiranje, filtriranje i čišćenje podataka, na način da nadopunjuje nepotpune i neprecizne podatke, obrađuje ih te izvodi zaključke, što ju čini nezaobilaznom u opisanim slučajevima (Watkins et al., 2003).

Lokanan u sklopu svog istraživanja testira preciznost i predviđanja raznih modela baziranih na strojnom učenju te ističe njihov postotak uspješnosti iznad 75%, dok za model baziran na neuronskoj mreži navodi još bolje rezultate, s preciznošću detekcije transakcija uključenih u pranje novca do 87%.

Drugo istraživanje preciznosti algoritama strojnog učenja provodi Faraji na javno dostupnom skupu podataka od 284.807 transakcija, od kojih su 492 potvrđene sumnjivim, odnosno njih 0,173%. Faraji opisan skup podataka analizira raznim metodama detekcije transakcija uključenih u pranje novca i tvrdi da je preciznost stabla odlučivanja (indukcijski algoritam) 77%, logističke regresije 90%, a neuronske mreže 91%. Naglašava činjenicu da je istraživanje provedeno na podacima samo jedne financijske institucije i da se rezultati ne mogu generalizirati za sve banke i financijske institucije.

Lokanan navodi da algoritmi strojnog učenja postižu dobre rezultate u identificiranju i označavanju transakcija pranja novca, da također mogu obavljati ulogu kontinuiranog ažuriranja rizika pranja novca za svakog klijenta te potiče njihovu daljnju uporabu.

Primjene strojnog učenja za potrebe borbe protiv pranja novca mogu se sumirati kroz domene:

- otkrivanja sumnjivih transakcija, kategorija koja pokriva pristupe koji nastoje identificirati sumnjive transakcije primjenom različitih metodologija i tehnika
- detekcije uzoraka i anomalija koje stvara pranje novca, kategorija koja pokriva pristupe koji djeluju otkrivanjem i klasificiranjem obrazaca prisutnim u analiziranim podacima
- procjene i analiza rizika, koja pokriva pristupe koji primjenjuju tehnike ocjenjivanja rizika od pranja novca provođenjem procjena ili analiza
- poboljšanje sigurnosti, kontrole, strukturiranja i/ili upravljanja cjelokupnih sustava
- primjene vizualnih tehnika za reprezentaciju podataka (Leite, 2019).

U kontekstu pranja novca, u praksi su uočene tri glavne prednosti korištenja tehnika strojnog učenja i rudarenja podataka. Prvo je značajno smanjenje količine utrošenog vremena na ručno pretraživanje i analiziranje velikih skupova podataka u potrazi za uzorcima i sumnjivim transferima. Druga prednost je rješavanje problema nedostatka radne snage, koji je usko povezan s problemom kratkih vremenskih rokova u istragama pranja novca. Korištenje tehnika strojnog učenja i rudarenja podataka olakšava brzo i precizno identificiranje tragova i obrazaca sumnjivih aktivnosti te zahtijeva brojčano manje jedinice stručnjaka, koje su specijalizirane i dobro obučene. Treća potencijalna korist je pravovremena identifikacija novih tragova pranja novca (Watkins et al., 2003), u kojoj sferi se ističu neuronske mreže koje su u mogućnosti pronalaska obrazaca koje čovjek vjerojatno ne bi uspio pronaći. Dodatno, navedene metodologije naknadno mogu generirati standardizirane izvještaje spremne za pregled financijskih istražitelja.

S druge strane, strojno učenje i rudarenje podataka donosi i određena ograničenja. Prvo, zahtijeva financiranje u obliku troškova razvitka i održavanja sustava, kao i troškove obuke specijaliziranih radnika koji će interpretirati rezultate modela. Primjerice, metodologije neizrazite logike i neuronskih mreža zahtijevaju opsežno istraživanje tematike prije početka razvojnog procesa, kao i dodatno vrijeme uloženo u podešavanje i učenje modela. Ipak, uz njihovu pravilnu primjenu, u konačnici je razumno očekivati da će se uloženo isplatiti i da će krajnji sustav biti učinkovitiji i višestruko nadoknaditi uloženo vrijeme.

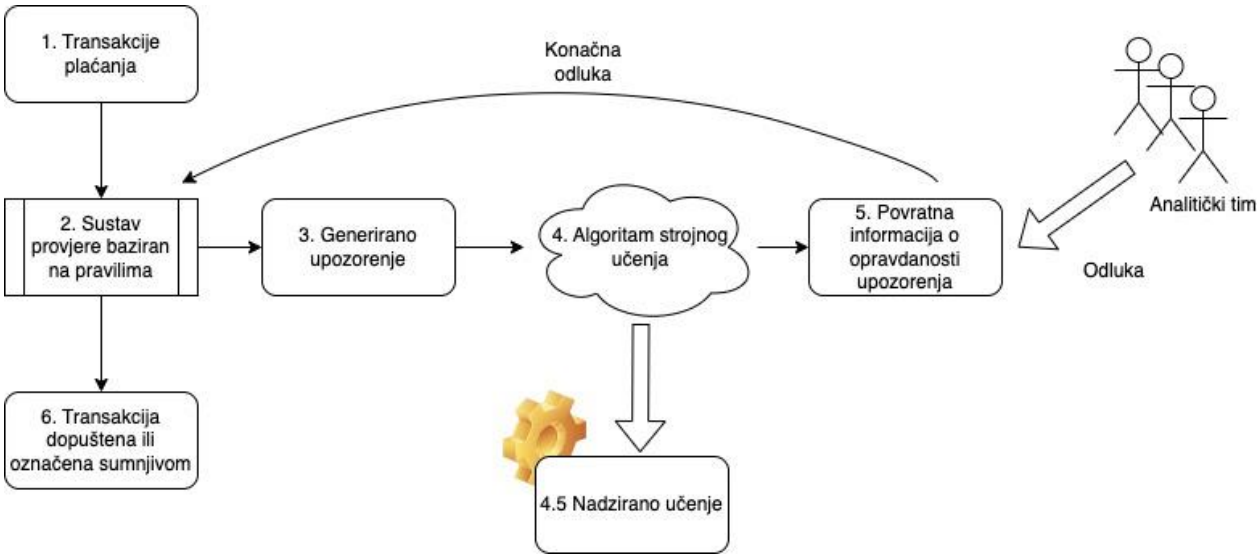
Drugo potencijalno ograničenje je izravno povezano s dostupnošću podataka potrebnih za pronalazak tragova pranja novca i prepoznavanja obrazaca sumnjivih aktivnosti. Ne dijeljenje

podataka na lokalnoj, regionalnoj, nacionalnoj i internacionalnoj razini stvara prepreke lakšem razvitku ovih tehnologija, no valja naglasiti da je napredak vidljiv na temelju poticaja internacionalnih organizacija kao što je Grupa za financijsku akciju protiv pranja novca (FATF).

Taj će se napredak pokazati kritičnim za financijske istražitelje koji žele koristiti alate strojnog učenja i rudarenja podataka za poboljšanje procesa detekcije pranja novca. Naime, u slučaju nedostupnosti dovoljno velikog skupa podataka s poznatim obrascima pranja novca, istraživači su primorani koristiti manje i nepotpune skupove podataka za obuku modela, što rezultira nižom preciznošću. Konačno, prepreka koja se mora savladati je nespremnost mijenjanja tradicionalnog načina poslovanja određenih subjekata zbog nedostatka razumijevanja (Watkins et al., 2003).

U nastavku se opisuje jedan od mogućih načina funkcioniranja modernog sustava detekcije pranja novca. Ideja je inkorporirati strojno učenje kao dodatnu razinu provjere i sigurnosti u već korišteni, postojeći sustav detekcije baziran na pravilima, kao što je model prezentiran u poglavlju 4.2. ovog rada, time smanjujući količinu lažno pozitivnih rezultata i poboljšavajući kvalitetu generiranih upozorenja (Infosys, 2019). Shema opisanog sustava prikazana je na slici 2.

Slika 2 Shema modernog sustava detekcije sumnjivih bankovnih transakcija



Izvor: izrada autora prema Infosys, 2019.

Proces počinje kad korisnik inicira provedbu određene transakcije, koja prije njenog izvršenja prolazi kroz sustav provjere baziran na pravilima. U slučaju da sustav ne generira upozorenje, transakcija se izvršava. U suprotnom transakciju, zajedno sa njenim cijelim kontekstom i popratnim informacijama koje su dostupne, dodatno provjerava i algoritam strojnog učenja,

koji daje svoju procjenu u obliku postotka (Lokanan, 2022), ako i strojno učenje sa dovoljnom sigurnošću potvrdi sumnju da se radi o pranju novca, upozorenje dolazi do analitičkog tima, koji donosi konačnu odluku treba li na temelju transakcije podnijeti izvješće o sumnjivim aktivnostima, u suprotnom se transakcija propušta i izvršava. Konačno, sam proces automatski strojnom učenju pruža nove podatke koje može analizirati, na temelju kojih postaje preciznije za buduće slučajeve (Watkins et al., 2003).

5. ZAKLJUČAK

Pranje novca je pretvaranje prihoda stečenih kriminalnim radnjama u imovinu koja je naizgled proizašla iz legitimnih izvora (Seymour, 2008). Ilegalnim je proglašeno prije 40-ak godina, potaknuto slučajevima kada se do kriminalaca nije moglo doći izravno. U kontekstu globalizacije svijeta i sve većeg povezivanja financijskih tržišta, vidljivo kroz rast broja i vrijednosti međunarodnih transfera, pranje novca postaje globalni problem. Procjene navode da je godišnja vrijednost opranog novca na svjetskoj razini između 2 i 5% svjetskog BDP-a, odnosno 800 milijardi do 2 bilijuna dolara godišnje (UNODC, 2022).

Pranje novca sastoji se od tri faze, faze polaganja, prikrivanja i integracije. Najranjivije i najpodložnije otkrivanju je u prvoj fazi, kada se novac prvi put uvodi u financijski sustav, obično kroz banke (HANFA, 2015), zbog čega je regulacija primorala financijske institucije da razviju sustave otkrivanja pranja novca i izvještavaju javne agencije. Sustavi u pitanju primarno funkcioniraju na temelju skupova pravila koja određuju je li transakcija sumnjiva ili nije. Pravila su brojna, a svode se na označavanje transakcija iznad određene vrijednosti, transakcija sa drugim rizičnim računima i državama, kao i transakcija koje odskaču od uobičajenih aktivnosti računa (Fong, 2022). U sklopu rada razrađena je funkcionalna verzija opisanog sustava te je na testnom skupu od nasumično generiranih 10.000 transakcija sumnjivim označila njih 119.

Prepoznati nedostatak sustava baziranih na pravilima je nedovoljna preciznost, odnosno generiranje lažnih pozitiva (Demetis, 2018), zbog čega ih najsuvremeniji bankovni sustavi nastoje nadograditi korištenjem tehnika rudarenja podataka i strojnog učenja. Navedene su u mogućnosti obraditi ogromne količine podataka te u njima pronaći obrasce i povezanosti, time olakšavajući otkrivanje pranja novca, dok je strojno učenje sposobno i automatski primijeniti zaključke iz prošlih skupova podataka na nove skupove. Najpreciznijima su se pokazale neuronske mreže, s uspješnošću otkrivanja slučaja pranja novca do 90% (Lokanan, 2022, Faraji, 2022), čime istražiteljima pružaju dodatnu dimenziju informacija korisnih u donošenju konačne odluke o potrebi podnošenja izvještaja o sumnjivoj transakciji nadležnim institucijama.

POPIS LITERATURE

Baker, R. (1999.), The biggest loophole in the free-market system, Washington Quarterly (22), 29–46, preuzeto s https://doi.org/10.1080/01636609909550422 [1.2.2023]

Barbey, R., Dab, S., Newman, H., Raymaekers, W. i Senant, , Y. (2017.), International payments: accelerating banks' transformation, preuzeto s https://www.swift.com/news-events/white-papers?category%5B0%5D=168546&category%5B1%5D=168551&category%5B2%5D=168581 [5.11.2022]

Basel Institute on Governance (2022.), Basel AML Index 2022: Ranking money laundering and terrorist financing risks around the world, preuzeto s https://baselgovernance.org/publications/basel-aml-index-2022 [1.11.2022]

Basel Institute on Governance (2022.), Global money laundering risk ranking, expert edition [podatkovni dokument], preuzeto s https://index.baselgovernance.org/ranking [14.12.2022]

Bhambri, V. (2011.), Application of Data Mining in Banking Sector, International Journal of Computer Science and Technology (2), preuzeto s http://www.ijcst.com/vol22/1/vivek.pdf [27.1.2023]

Chedrawi, C., Atallah, Y., Osta, S. (2020.), Big Data in the Banking Sector from a Transactional Cost Theory (TCT) Perspective - The Case of Top Lebanese Banks, preuzeto s https://doi.org/10.1007/978-3-030-34269-2_27 [28.1.2023]

Cindori, S. (2007.), The Money Laundering Prevention System, Financial theory and practice, 31 (1), 59-76, preuzeto s https://hrcak.srce.hr/16380 [1.11.2022]

Demetis, D. S., (2018.), Fighting money laundering with technology: A case study of Bank X in the UK, Decision Support Systems (105), 96–107, preuzeto s https://doi.org/10.1016/j.dss.2017.11.005 [27.1.2023]

Digital Adoption, (2022.), Digital Banking Adoption: Everything You Need To Know, preuzeto s https://www.digital-adoption.com/digital-banking-adoption [23.12.2022]

Direktiva Europskog parlamenta i vijeća o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma (2015.), 2015/849, preuzeto s https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849 [7.12.2022]

Dong, L. i Tjortjis, C. (2003.), Experiences of Using a Quantitative Approach for Mining Association Rules, Lecture Notes in Computer Science (2690), preuzeto s https://doi.org/10.1007/978-3-540-45080-1_93 [27.1.2023]

ECB (2022.), Payments statistics: methodological notes, preuzeto s https://sdw.ecb.europa.eu/servlet/desis?node=1000002018 [21.1.2023]
Empact (2021.), General Factsheet — Operational Action Plans (OAPS), preuzeto s https://www.consilium.europa.eu/media/50206/combined-factsheets.pdf [31.1.2023]
Eur-Lex (2016.), Opća uredba o zaštiti podataka, preuzeto s https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 [21.1.2023]
Europol (2022), EU Policy Cycle - Empact, preuzeto s https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact [31.1.2023]
Europska Komisija (2022.), High risk third countries and the International context content of anti-money laundering and countering the financing of terrorism, preuzeto s https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en [16.1.2023]
Europska Komisija (2022.), ICT sector analysis, Data & metadata 2022 [podatkovni dokument], preuzeto s https://joint-research-centre.ec.europa.eu/predict/ict-sector-analysis-2022/data-metadata-2022_en [6.1.2023]
Eurostat (2022.), ICT sector - value added, employment and R&D, preuzeto s https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_sector_-_value_added,_employment_and_R%26D#The_size_of_the_ICT_sector_as_measured_by_value_added [6.1.2023]
Eurostat (2022.), Individuals using the internet for internet banking [podatkovni dokument], preuzeto s https://ec.europa.eu/eurostat/databrowser/view/TIN00099/default/table?lang=en&category=isoc.isoc_i.isoc_iiu [1.11.2022]
Eurostat (2013.), Money laundering in Europe, preuzeto s https://ec.europa.eu/eurostat/en/web/products-statistical-working-papers/-/ks-tc-13-007 [7.12.2022]
Faraji, Z. (2022.), A Review of Machine Learning Applications for Credit Card Fraud Detection with A Case study, Seisense Journal of Management, preuzeto s https://doi.org/10.33215/sjom.v5i1.770 [3.11.2022]
FATF (2022.), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, preuzeto s www.fatf-gafi.org/recommendations.html [1.11.2022]

Financial Crimes Enforcement Network (2003.), Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative, preuzeto s https://www.fincen.gov/sites/default/files/shared/sarnarrcompletguidfinal_112003.pdf [14.1.2023]

Fong, J. (2022.) Transaction Monitoring Software: How It Works and Tips on Deploying It, preuzeto s https://seon.io/resources/transaction-monitoring-software-how-it-works-and-tips/ [3.12.2022]

Garcia, E., Romero, C., Ventura, S., i Calders, T. (2008.), Drawbacks and solutions of applying association rule mining in learning management systems, preuzeto s https://ceur-ws.org/Vol-305/paper02.pdf [27.1.2023]

Gyeni-Boateng, R. (2020.), The Role of Tax Haven in Money Laundering Activities, preuzeto s https://www.linkedin.com/pulse/role-tax-haven-money-laundering-activities-richieson/ [13.12.2022]

Hagenlocher, P. (2017.), Decision Tree Learning, preuzeto s https://www5.in.tum.de/lehre/seminare/datamining/ss17/paper_pres/08_decision_tree/paper.pdf [30.1.2023]

HANFA (2015.), Smjernice za provođenje Zakona o sprječavanju pranja novca i financiranja terorizma za obveznike u nadležnosti Hrvatske agencije za nadzor financijskih usluga. Zagreb, preuzeto s https://www.hanfa.hr/uploads/2015/01/23/1422021093_467106ed6c18b88b8a32ee8cb3463175.pdf [1.11.2022]

Hines, R. J. (2007.), Tax Havens, preuzeto s https://www.bus.umich.edu/otpr/WP2007-3.pdf [13.12.2022]

Hunady, J., Pisar, P. i Durcekova, I. (2019.), Business R&D Expenditure in the ICT Sector: Effects on Business Performance Indicators, 445-456, preuzeto s https://hrcak.srce.hr/251039 [7.1.2023]

Infosys (2019.), Application Of Machine Learning In Aml Transaction Filtering, preuzeto s https://www.infosys.com/industries/financial-services/insights/documents/aml-transaction-filtering.pdf [29.1.2023]

Javapoint, (2021a), Data Mining Tools, preuzeto s https://www.javatpoint.com/data-mining-tools [28.1.2023]

Javapoint (2021b), Artificial Intelligence (AI) Tutorial, preuzeto s https://www.javatpoint.com/artificial-intelligence-ai [28.1.2023]

Javapoint (2021c), Machine Learning Tutorial, preuzeto s https://www.javatpoint.com/machine-learning [29.1.2023]
Javapoint (2021d), Artificial Neural Network Tutorial, preuzeto s https://www.javatpoint.com/artificial-neural-network [29.1.2023]
Kullaya S., A. i Sarojamma, B. (2020.), Bank transaction data modeling by optimized hybrid machine learning merged with ARIMA, preuzeto s https://doi.org/10.1080/23270012.2020.1726217 [21.1.2023]
Leite, S. G. (2019.), Application of Technological Solutions in the Fight Against Money Laundering-A Systematic Literature Review, preuzeto s https://www.mdpi.com/2076-3417/9/22/4800 [3.11.2022]
Lokanan, E. M. (2022.), Predicting Money Laundering Using Machine Learning and Artificial Neural Networks Algorithms in Banks, preuzeto s https://doi.org/10.1080/19361610.2022.2114744 [29.1.2023]
Ministarstvo financija (2021.), Godišnje izvješće o radu ureda za 2020. godinu. Zagreb. preuzeto s https://mfin.gov.hr/UserDocsImages//dokumenti/o-ministarstvu/ustrojstvo//Godisnje%20izvjesce%20o%20radu%20Ureda%20za%202020.%20godinu.pdf [2.11.2022]
Mugarura, N. (2017.), Tax havens, offshore financial centres and the current sanctions regimes, Journal of Financial Crime, 24 (2), 200-222, preuzeto s https://doi.org/10.1108/JFC-01-2016-0008 [13.12.2022]
Muller, W., Kalin, C., Goldsworth, J., Anti-Money Laundering: International Law and Practice, England, John Willey & Sons Ltd
Musoko, J. (2020.), Data models for Financial Transactions, preuzeto s https://www.jessym.com/articles/data-models-for-financial-transactions [21.1.2023]
National Infrastructure Commission (2022.), NIA2 Baseline report: charts data-set [podatkovni dokument], preuzeto s https://nic.org.uk/data/all-data/nia2-baseline-charts/ [7.1.2023]
OECD (2022.), Individuals using the Internet (% of population) [podatkovni dokument], preuzeto s https://data.worldbank.org/indicator/IT.NET.USER.ZS [23.12.2022]
OECD (2020.), Compare your income – Methodology and conceptual issues, preuzeto s https://www.oecd.org/statistics/Compare-your-income-methodology.pdf [23.12.2022]
OECD Going Digital Toolkit (2022.), ICT investment as a share of GDP, preuzeto s https://goingdigital.oecd.org/indicator/30 [7.11.2023]

Ostapchenya, D. (2021.), The Role of Big Data in Banking : How do Modern Banks Use Big Data, preuzeto s https://www.finextra.com/blogposting/20446/the-role-of-big-data-in-banking--how-do-modern-banks-use-big-data [27.1.2023]

Pezer Blečić, S. (2014.), Aktualnosti u području sprječavanja pranja novca i financiranja terorizma (promjena međunarodnog regulatornog okvira), Zagreb, Hrvatska gospodarska komora, preuzeto s http://www.agenti.hr/sadrzaj/info-agent/strukovni-forumi/forum-23/23-forum-Aktualnosti_ZSPNFT-Promjena_medunarodnog_regulatornog_okvira.pdf [3.11.2022]

Rocha-Salazar, J., Segovia-Vargas, M. i Camacho-Miñano, M. (2021), Money laundering and terrorism financing detection using neural networks and an abnormality indicator, preuzeto s https://doi.org/10.1016/j.eswa.2020.114470 [30.1.2023]

Scott, I., Svinterikou, S., Tjortjis, C., Keane, A. (1998.), Experiences of using Data Mining in a Banking Application, preuzeto s https://www.ihu.edu.gr/tjortjis/Experiences%20of%20using%20Data%20Mining%20in%20a%20Banking%20Application.pdf [27.1.2023]

Scott, V., S. i Zachariadis, M. (2012.), Origins and Development of SWIFT, 1973– 2009, preuzeto s https://eprints.lse.ac.uk/46490/1/Origins%20and%20Development%20of.pdf [9.1.2023]

Seymour, B. (2008.), Global Money Laundering, Journal of Applied Security Research, (3), 373-387, preuzeto s https://doi.org/10.1080/19361610801981001 [30.1.2023]

SEON (2022.), Guide to Fraud Monitoring and Fraud Alerts, preuzeto s https://seon.io/resources/guides/fraud-monitoring-and-fraud-alerts/#h-trigerring-alerts-and-actions [14.1.2023]

Srivastava, U. i Gopalkrishnan, S. (2015.), Impact of Big Data Analytics on Banking Sector: Learning for Indian Banks, Procedia Computer Science (50), 643–652 preuzeto s https://doi.org/10.1016/j.procs.2015.04.098 [27.1.2023]

Swift (2022.) Swift Annual Review 2021, preuzeto s https://www.swift.com/news-events/publications?category%5B0%5D=168606 [12.1.2023]

Swift (2020.), SWIFT gpi, Driving a payments revolution, preuzeto s https://www.swift.com/news-events/publications?category%5B0%5D=168606 [30.1.2023]

Unger, B. i van der Linde, D. (2013). Research Handbook on Money Laundering, preuzeto s https://doi.org/10.4337/9780857934000 [6.12.2022]

UNODC, (2022.), Money Laundering, preuzeto s https://www.unodc.org/unodc/en/money-laundering/overview.html [1.2.2023]

Villányi, B. (2021.) Money Laundering: History, Regulations, and Techniques, Oxford Research Encyclopedia of Criminology, preuzeto s https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-708 [6.12.2022]

Watkins, R. C., Reynolds, K. M., Demara, R., Georgiopoulos, M., Gonzalez, A. i Eaglin, R. (2003.), Tracking dirty proceeds: Exploring data mining technologies as tools to investigate money laundering, Police Practice and Research, 4(2), 163–178 preuzeto s https://doi.org/10.1080/15614260308020 [29.1.2023]

Takats, E. (2007), A theory of "crying wolf": the economics of money laundering enforcement, IMF Working Paper 07/81, preuzeto s https://www.imf.org/external/pubs/ft/wp/2007/wp0781.pdf [12.12.2022]

Tax Justice Network (2022.), Financial Secrecy Indeks 2022 [podatkovni dokument], preuzeto s https://fsi.taxjustice.net/#/ [15.12.2022]

Tax Justice Network (2018.), Financial Secrecy affecting the European Union: Patterns across member states, and what to do about it, preuzeto s https://taxjustice.net/reports/the-bilateral-financial-secrecy-index/ [22.12.2022]

Teichmann, F.M. (2019.), Recent trends in money laundering and terrorism financing, Journal of Financial Regulation and Compliance, (27), 2-12, preuzeto s https://doi.org/10.1108/JFRC-03-2018-0042 [30.1.2023]

Zakon o sprječavanju pranja novca i financiranja terorizma, Narodne novine NN 108/17, 39/19 (2017.), preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/2017_11_108_2488.html [1.11.2022]

Popis tablica

Popis slika

Prilozi

Prilog 1. Opis procesa generiranja fiktivnih bankovnih računa i transakcija za potrebe modela

Za potrebe testiranja modela predloženog u radu, napravljen je program koji nasumičnim putem generira proizvoljan broj transakcija. Korišten je programski jezik Java, programski jezik opće namjene i visokih mogućnosti, razvijen 1995. godine (Singh, 2022.). Korišten je u kombinaciji sa Spring Boot-om, tehnologijom koja nadopunjuje Javu na način da za određene probleme nudi unaprijed napravljena programska rješenja kojima ubrzava i olakšava stvaranje samostalnih aplikacija (Spring, 2022.).

Transakcije su generirane slučajnom šansom, što u dovoljno velikom broju iteracija omogućuje stvaranje velikog broja različitih slučaja, s idejom da se što bolje imitira ponašanje stvarnih korisnika koji koriste bankovne sustave za svakodnevne transakcije plaćanja. Generirane transakcije spremljene su u bazu podataka te naknadno izvedene u tablicu radi bolje vizualizacije.

S ciljem pribavljanja što reprezentativnijih podataka, gdje je bilo moguće, šanse za generiranjem određene vrste transakcije prilagođene su prema statističkim podacima, dok se u ostalim slučajima koristila subjektivna procjena, no, valja naglasiti da je za sam prikaz funkcioniranja modela to suvišno. Udio kartičnih transakcija sa inozemstvom u ukupnom broju kartičnih plaćanja u 2022. bio 8% (izračunato prema HNB, 2022.). Broj zaprimljenih obavijesti o sumnjivim gotovinskim transakcijama u 2019. godini je bio 56.701 (Ministarstvo financija, 2021.), dok je ukupni broj transakcija uplate i isplate gotovine u 2022. godini bio 27.584.870, pa je mogućnost da se generira transakcija iznad 10.000 eura stavljena kao 0,21% (relevantno za prvo pravilo modela).

Literatura prilog 1.

HNB (2022.), Izdavanje platnih instrumenata, preuzeto s https://www.hnb.hr/statistika/statisticki-podaci/platne-usluge/izdavanje-platnih-instrumenata [19.1.2023]

Ministarstvo financija (2021.), Godišnje izvješće o radu ureda za 2020. godinu. Zagreb. preuzeto s https://mfin.gov.hr/UserDocsImages//dokumenti/o-ministarstvu/ustrojstvo//Godisnje%20izvjesce%20o%20radu%20Ureda%20za%202020.%20godinu.pdf [2.11.2022]

Singh, K. (2022.), Introduction to Java, preuzeto s https://www.scaler.com/topics/java/introduction-to-java/ [19.1.2023]

Spring (2022.) Spring Boot, preuzeto s https://spring.io/projects/spring-boot [19.1.2023]

Prilog 2. Tablica generiranih bankovnih transakcija prvih pet korisničkih računa (cijela tablica dostupna na zahtjev)

id transakcije	korisnikov id	tip transakcije	datum	iznos	saldo nakon transakcije	država drugog korisnika	visokorizična država	transferirano sa/na sumnjiv račun	razlog za sumnju	sumnjiva
1	1	lokalni transfer sa drugog računa	21.01.2021	136	74.349	x	NE	NE	x	NE
2	1	gotovinska isplata	25.01.2021	620	73.729	x	NE	NE	x	NE
3	1	lokalni transfer na drugi račun	26.01.2021	275	73.454	x	NE	NE	x	NE
4	1	lokalni transfer sa drugog računa	31.01.2021	693	74.147	x	NE	NE	x	NE
5	1	gotovinska isplata	31.01.2021	853	73.294	x	NE	NE	x	NE
6	1	lokalni transfer na drugi račun	02.02.2021	176	73.118	x	NE	NE	x	NE
7	1	lokalni transfer sa drugog računa	07.02.2021	46	73.164	x	NE	NE	x	NE
8	1	lokalni transfer na drugi račun	10.02.2021	220	72.944	x	NE	NE	x	NE
9	1	gotovinska uplata	14.02.2021	62	73.006	x	NE	NE	x	NE
10	1	lokalni transfer sa drugog računa	16.02.2021	47	73.053	x	NE	NE	x	NE
11	1	gotovinska uplata	23.02.2021	101	73.154	x	NE	NE	x	NE
12	1	gotovinska uplata	28.02.2021	50	73.204	x	NE	NE	x	NE
13	1	lokalni transfer sa drugog računa	07.03.2021	256	73.460	x	NE	NE	x	NE
14	1	lokalni transfer na drugi račun	11.03.2021	14	73.446	x	NE	NE	x	NE
15	1	lokalni transfer na drugi račun	13.03.2021	3.589	69.857	x	NE	NE	x	NE
16	1	lokalni transfer sa drugog računa	19.03.2021	82	69.939	x	NE	NE	x	NE
17	1	gotovinska uplata	22.03.2021	40	69.979	x	NE	NE	x	NE
18	1	gotovinska isplata	28.03.2021	245	69.734	x	NE	NE	x	NE
19	1	lokalni transfer sa drugog računa	30.03.2021	186	69.920	x	NE	NE	x	NE
20	1	lokalni transfer na drugi račun	04.04.2021	251	69.669	x	NE	NE	x	NE
21	1	gotovinska isplata	09.04.2021	177	69.492	x	NE	NE	x	NE

22	1	lokalni transfer na drugi račun	13.04.2021	299	69.193	x	NE	NE	x	NE
23	1	gotovinska isplata	16.04.2021	605	68.588	x	NE	NE	x	NE
24	1	lokalni transfer sa drugog računa	21.04.2021	240	68.828	x	NE	NE	x	NE
25	1	lokalni transfer sa drugog računa	21.04.2021	7.495	76.323	x	NE	NE	x	NE
26	1	gotovinska isplata	25.04.2021	1.243	75.080	x	NE	NE	x	NE
27	1	lokalni transfer na drugi račun	25.04.2021	8	75.072	x	NE	NE	x	NE
28	1	gotovinska uplata	26.04.2021	180	75.252	x	NE	NE	x	NE
29	1	gotovinska isplata	02.05.2021	4.018	71.234	x	NE	NE	x	NE
30	2	gotovinska isplata	25.01.2021	137	65.152	x	NE	NE	x	NE
31	2	gotovinska uplata	28.01.2021	28	65.180	x	NE	NE	x	NE
32	2	gotovinska uplata	30.01.2021	242	65.422	x	NE	NE	x	NE
33	2	gotovinska uplata	05.02.2021	149	65.571	x	NE	NE	x	NE
34	2	lokalni transfer na drugi račun	08.02.2021	292	65.279	x	NE	NE	x	NE
35	2	gotovinska uplata	08.02.2021	3	65.282	x	NE	NE	x	NE
36	2	lokalni transfer na drugi račun	11.02.2021	131	65.151	x	NE	NE	x	NE
37	2	lokalni transfer na drugi račun	17.02.2021	546	64.605	x	NE	NE	x	NE
38	2	lokalni transfer sa drugog računa	24.02.2021	249	64.854	x	NE	NE	x	NE
39	2	lokalni transfer sa drugog računa	02.03.2021	0	64.854	x	NE	NE	x	NE
40	2	gotovinska uplata	05.03.2021	29	64.883	x	NE	NE	x	NE
41	2	gotovinska isplata	06.03.2021	177	64.706	x	NE	NE	x	NE
42	2	lokalni transfer na drugi račun	12.03.2021	3.452	61.254	x	NE	NE	x	NE
43	2	gotovinska isplata	14.03.2021	20	61.234	x	NE	NE	x	NE
44	2	lokalni transfer sa drugog računa	21.03.2021	58	61.292	x	NE	NE	x	NE
45	2	lokalni transfer sa drugog računa	21.03.2021	126	61.418	x	NE	NE	x	NE
46	2	gotovinska isplata	24.03.2021	746	60.672	x	NE	NE	x	NE
47	2	lokalni transfer na drugi račun	29.03.2021	176	60.496	x	NE	NE	x	NE
48	2	lokalni transfer na drugi račun	31.03.2021	1.689	58.807	x	NE	NE	x	NE
49	2	lokalni transfer sa drugog računa	03.04.2021	193	59.000	x	NE	NE	x	NE

50	2	lokalni transfer na drugi račun	04.04.2021	186	58.814	x	NE	NE	x	NE
51	2	gotovinska uplata	10.04.2021	300	59.114	x	NE	NE	x	NE
52	2	lokalni transfer na drugi račun	13.04.2021	116	58.998	x	NE	NE	x	NE
53	2	lokalni transfer na drugi račun	14.04.2021	56	58.942	x	NE	NE	x	NE
54	2	gotovinska isplata	18.04.2021	208	58.734	x	NE	NE	x	NE
55	2	gotovinska isplata	19.04.2021	69	58.665	x	NE	NE	x	NE
56	2	lokalni transfer na drugi račun	20.04.2021	165	58.500	x	NE	NE	x	NE
57	2	lokalni transfer sa drugog računa	23.04.2021	241	58.741	x	NE	NE	x	NE
58	2	internacionalni transfer sa drugog rač.	28.04.2021	19	58.760	Portugal	NE	NE	x	NE
59	2	gotovinska uplata	30.04.2021	81	58.841	x	NE	NE	x	NE
60	2	gotovinska isplata	02.05.2021	16	58.825	x	NE	NE	x	NE
61	2	gotovinska uplata	08.05.2021	84	58.909	x	NE	NE	x	NE
62	3	gotovinska uplata	23.01.2021	160	58.881	x	NE	NE	x	NE
63	3	gotovinska isplata	28.01.2021	38	58.843	x	NE	NE	x	NE
64	3	lokalni transfer sa drugog računa	31.01.2021	92	58.935	x	NE	NE	x	NE
65	3	lokalni transfer sa drugog računa	05.02.2021	263	59.198	x	NE	NE	x	NE
66	3	lokalni transfer sa drugog računa	09.02.2021	94	59.292	x	NE	NE	x	NE
67	3	lokalni transfer sa drugog računa	14.02.2021	3	59.295	x	NE	NE	x	NE
68	3	gotovinska isplata	16.02.2021	249	59.046	x	NE	NE	x	NE
69	3	lokalni transfer na drugi račun	19.02.2021	136	58.910	x	NE	NE	x	NE
70	3	gotovinska isplata	23.02.2021	27	58.883	x	NE	NE	x	NE
71	3	lokalni transfer na drugi račun	24.02.2021	167	58.716	x	NE	NE	x	NE
72	3	gotovinska isplata	26.02.2021	79	58.637	x	NE	NE	x	NE
73	3	internacionalni transfer sa drugog rač.	27.02.2021	97	58.734	Antarktika	NE	NE	x	NE
74	3	internacionalni transfer na drugi rač.	05.03.2021	703	58.031	Sv. Marten	NE	NE	x	NE
75	3	lokalni transfer na drugi račun	08.03.2021	168	57.863	x	NE	NE	x	NE
76	3	gotovinska isplata	09.03.2021	344	57.519	x	NE	NE	x	NE

77	3	lokalni transfer na drugi račun	14.03.2021	165	57.354	x	NE	NE	x	NE
78	3	gotovinska uplata	18.03.2021	191	57.545	x	NE	NE	x	NE
79	3	lokalni transfer sa drugog računa	24.03.2021	197	57.742	x	NE	NE	x	NE
80	3	gotovinska uplata	27.03.2021	208	57.950	x	NE	NE	x	NE
81	3	internacionalni transfer na drugi rač.	02.04.2021	281	57.669	Filipini	DA	NE	visokorizična zemlja	DA
82	3	lokalni transfer na drugi račun	03.04.2021	4.529	53.140	x	NE	NE	x	NE
83	3	gotovinska uplata	07.04.2021	184	53.324	x	NE	NE	x	NE
84	3	gotovinska uplata	10.04.2021	152	53.476	x	NE	NE	x	NE
85	3	gotovinska uplata	11.04.2021	36	53.512	x	NE	NE	x	NE
86	3	lokalni transfer sa drugog računa	17.04.2021	295	53.807	x	NE	NE	x	NE
87	3	lokalni transfer na drugi račun	23.04.2021	86	53.721	x	NE	NE	x	NE
88	3	gotovinska isplata	23.04.2021	7.335	46.386	x	NE	NE	x	NE
89	3	lokalni transfer sa drugog računa	28.04.2021	300	46.686	x	NE	NE	x	NE
90	3	lokalni transfer sa drugog računa	30.04.2021	277	46.963	x	NE	NE	x	NE
91	3	gotovinska isplata	01.05.2021	181	46.782	x	NE	NE	x	NE
92	3	gotovinska uplata	03.05.2021	177	46.959	x	NE	NE	x	NE
93	3	lokalni transfer sa drugog računa	05.05.2021	144	47.103	x	NE	NE	x	NE
94	3	internacionalni transfer na drugi rač.	11.05.2021	85	47.018	Afganistan	DA	NE	visokorizična zemlja	DA
95	3	gotovinska uplata	13.05.2021	42	47.060	x	NE	NE	x	NE
96	4	lokalni transfer na drugi račun	25.01.2021	1.854	58.157	x	NE	NE	x	NE
97	4	gotovinska isplata	27.01.2021	251	57.906	x	NE	NE	x	NE
98	4	lokalni transfer na drugi račun	03.02.2021	1.209	56.697	x	NE	NE	x	NE
99	4	lokalni transfer na drugi račun	06.02.2021	353	56.344	x	NE	NE	x	NE
100	4	gotovinska uplata	13.02.2021	94	56.438	x	NE	NE	x	NE
101	4	internacionalni transfer sa drugog rač.	19.02.2021	47	56.485	Njemačka	NE	NE	x	NE
102	4	gotovinska isplata	23.02.2021	195	56.290	x	NE	NE	x	NE
103	4	gotovinska isplata	01.03.2021	297	55.993	x	NE	NE	x	NE

104	4	lokalni transfer na drugi račun	06.03.2021	167	55.826	x	NE	NE	x	NE
105	4	gotovinska isplata	06.03.2021	217	55.609	x	NE	NE	x	NE
106	4	lokalni transfer sa drugog računa	10.03.2021	47	55.656	x	NE	NE	x	NE
107	4	gotovinska isplata	14.03.2021	123	55.533	x	NE	NE	x	NE
108	4	gotovinska uplata	17.03.2021	6.617	62.150	x	NE	NE	x	NE
109	4	lokalni transfer na drugi račun	17.03.2021	51	62.099	x	NE	NE	x	NE
110	4	lokalni transfer sa drugog računa	23.03.2021	570	62.669	x	NE	NE	x	NE
111	4	lokalni transfer sa drugog računa	27.03.2021	124	62.793	x	NE	NE	x	NE
112	4	lokalni transfer na drugi račun	02.04.2021	222	62.571	x	NE	NE	x	NE
113	4	lokalni transfer sa drugog računa	03.04.2021	121	62.692	x	NE	NE	x	NE
114	4	internacionalni transfer sa drugog rač.	08.04.2021	267	62.959	Irska	NE	NE	x	NE
115	4	lokalni transfer sa drugog računa	13.04.2021	68	63.027	x	NE	NE	x	NE
116	4	lokalni transfer sa drugog računa	14.04.2021	125	63.152	x	NE	NE	x	NE
117	4	internacionalni transfer sa drugog rač.	18.04.2021	101	63.253	Haiti	DA	NE	visokorizična zemlja	DA
118	4	lokalni transfer na drugi račun	19.04.2021	6.534	56.719	x	NE	NE	x	NE
119	4	gotovinska uplata	24.04.2021	493	57.212	x	NE	NE	x	NE
120	4	gotovinska uplata	29.04.2021	124	57.336	x	NE	NE	x	NE
121	4	gotovinska isplata	01.05.2021	263	57.073	x	NE	NE	x	NE
122	5	gotovinska uplata	20.01.2021	120	67.952	x	NE	NE	x	NE
123	5	gotovinska isplata	21.01.2021	117	67.835	x	NE	NE	x	NE
124	5	lokalni transfer na drugi račun	25.01.2021	300	67.535	x	NE	NE	x	NE
125	5	lokalni transfer sa drugog računa	30.01.2021	87	67.622	x	NE	NE	x	NE
126	5	lokalni transfer na drugi račun	01.02.2021	537	67.085	x	NE	NE	x	NE
127	5	gotovinska isplata	03.02.2021	221	66.864	x	NE	NE	x	NE
128	5	gotovinska uplata	07.02.2021	240	67.104	x	NE	NE	x	NE
129	5	lokalni transfer na drugi račun	08.02.2021	236	66.868	x	NE	NE	x	NE
130	5	gotovinska isplata	13.02.2021	36	66.832	x	NE	NE	x	NE

131	5	lokalni transfer na drugi račun	17.02.2021	2.382	64.450	x	NE	NE	x	NE
132	5	lokalni transfer sa drugog računa	19.02.2021	118	64.568	x	NE	NE	x	NE
133	5	gotovinska uplata	25.02.2021	205	64.773	x	NE	NE	x	NE
134	5	gotovinska uplata	27.02.2021	385	65.158	x	NE	NE	x	NE
135	5	gotovinska isplata	28.02.2021	295	64.863	x	NE	NE	x	NE
136	5	lokalni transfer na drugi račun	02.03.2021	6.937	57.926	x	NE	NE	x	NE
137	5	gotovinska isplata	04.03.2021	74	57.852	x	NE	NE	x	NE
138	5	gotovinska isplata	09.03.2021	110	57.742	x	NE	NE	x	NE

Životopis studenta

DARJAN BOŽIĆ

kontakt broj: +385 994364787
email: darjan.bozic.357@gmail.com
linkedin.com/in/darjan-bozic-b73213152
adresa: Dr. Vlatka Mačeka 37, 40 000 Čakovec, Hrvatska
datum rođenja: 01/03/1999
državljanstvo: hrvatsko
spol: muško

DIGITALNE VJEŠTINE

Java, Kotlin, Spring | MySQL | React, Javascript | napredno znanje MS Office-a (Excel - EdukaCentar certifikat, Word, Powerpoint) | google docs

JEZICI

Engleski: C2 (iskusni korisnik/native speaker level)
Njemački: B1 (samostalan korisnik)
Materinski jezik: Hrvatski

HOBIJI I INTERESI

- čitanje
- street workout
- planinarenje
- snowboarding
- programiranje
- financije

RADNO ISKUSTVO

Inženjer za razvoj softvera
CROZ | 2022/2023
Junior Revizor
KPMG Hrvatska | 2021/2022
Demonstrator
Ekonomski fakultet Zagreb. | 2019 - 2021

- Katedra za makroekonomiju i gospodarski razvoj
- Kolegij: Makroekonomija
- Tehnička podrška; Pomoć studentima pri savladavanju kolegija; Održavanje demonstratura u dvorani

OBRAZOVANJE

CROZ akcelerator | 2022

- Razvijanje aplikacije u Javi i React-u

Infinum Academy | 2021

- Razvijanje aplikacije u Spring-u i Kotlin-u

Integrirani preddiplomski i diplomski sveučilišni studij poslovna ekonomija, smjer Financije | 2017 - 2023

- Ekonomski fakultet Zagreb
- prosjek 4.5/5

Gimnazija Josipa Slavenskog Čakovec | 2013 - 2017
srednjoškolsko obrazovanje

PROJEKTI

Institutional Investors LAB
2020./2021.

- vodio tim studenata u kreaciji institucionalnog investitora
- proveo ekstenzivan pregled literature i regulacije za projekt
- sudjelovao u izradi investicijskog portfelja, prognoza
- financijskih izvještaja, distribucijskog i marketinškog plana

Young Entrepreneurs in Croatia
AIESEC | 2016.

- izradio detaljan koncept mobilne aplikacije za pomoć studentima s organizacijom vremena
- bio zadužen za timsku i projektnu koordinaciju

University trading tournament
Financijski klub Zagreb | 2018.

- sudjelovao u simulaciji trgovanja i investiranja na burzi korištenjem virtualnog novca