GOD. 2 . BR. 2 [2018] EDUKATIVNI ČASOPIS ZA BANKARSKI I FINANSIJSKI SEKTOR U BiH ISSN 2566-3100

FRAUDinfo

UDRUŽENJE PROFESIONALNIH RIZIK MENADŽERA U BOSNI I HERCEGOVINI

9 772566 310008

UPRMBiH
Udruženje profesionalnih rizik menadžera

Amir Softić
Predsjednik Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini

Amar Brkan
Generalni sekretar Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini

Dragi čitaoci!

Pred vama je drugo izdanje biltena koji se bavi vrstama, tehnikama, prevencijom i posljedicama prevarnih radnji koje su usmjerene prema finansijskim institucijama i njihovim klijentima. Prevare postaju globalni problem. Prema istraživanju ***Payment Fraud and Control Survey (AFP 2017.)***, skoro 50% ispitanika (organizacija) je prijavilo povećanje broja pokušaja prevarnih radnji.

Obrasci i metode se svakodnevno usavršavaju, a posljedice postaju sve značajnije. Zato razumijevanje važnosti upravljanja rizicima prevara postaje najvažniji elementi poslovanja subjekata finansijskih tržišta.

Godina 2017. nam je donijela koncentraciju prevarnih radnji na računima klijenata (account-centric attacks) i krađu personalnih podataka putem cyber kriminalnog djelovanja. Izvori podataka o personalnim podacima postaju najvrednija "aktiva" kriminalaca. Novi oblici napada mogu dovesti do značajnih finansijskih gubitaka i možda, još važnije, do gubitka povjerenja u finansijske institucije.

Na osnovu *Kaspersky Security Biltena* (Novembar 2017.), u 2018. godini možemo očekivati sve češće i organizovanije napade na real-time sisteme plaćanja, mobilne tehnologije, crypto valutne ciljeve, ATM-ove, kao i prodaju antifraud sistema koji sami po sebi imaju prevarnu komponentu i napade poznatije kao socijalni inžinjering. Sve ovo će neminovno dovesti do potrebe većih investicija i povećanja ukupnih troškova poslovanja finansijskih institucija koje će se susresti i sa brojnim regulatornim ograničenjima i izazovima.

Urednički tim časopisa *Fraud Info*, članovi Udruženja profesionalnih rizik menadžera u BiH (UPRM-BiH), svojim stručnim i istraživačkim člancima će pokušati pomoći finansijskim institucijama BiH da bolje razumiju rizike prevara i adekvatnije se zaštite od istih.

Vas, dragi čitaoci, pozivamo da nam se pridružite i kroz svoje sugestije, pitanja i prijedloge pomognete da ovaj bilten bude što kvalitetniji i sadržajniji. Sve vaše sugestije, pitanja i prijedloge možete slati na oficijelnu e-mail adresu UPRMBIH **amar.brkan@uprmbih.ba**.

Ovu priliku koristimo da se posebno zahvalimo našem partneru, Evropskom fondu za Jugoistočnu Evropu (EFSE), koji je podržao cjelokupan projekat i omogućio nam da *Fraud Info* bude distribuiran do vas i u 2018. godini!

UPRMBiH
Udruženje profesionalnih rizik menadžera

FRAUDinfo

Udruženje profesionalnih rizik menadžera u BiH

Zagrebačka 50/IV,
71 000 Sarajevo - BiH

tel.:
+387 62 393 568

e-mail:
amar.brkan@uprmbih.ba

Izdavač:
UDRUŽENJE
PROFESIONALNIH
RIZIK MENADŽERA

Design, DTP & Print:
PERFECTA, Sarajevo

perfecta

Branilaca Šipa 33

tel.:
+387 61 214 222

e-mail:
info@perfecta.ba

ISSN 2566-3100

UVODNA RIJEČ

FRAUD INFO

NOVA PLATFORMA ZA BORBU PROTIV PREVARA U FINANSIJSKOM SEKTORU

Autori:
Mujo Vilašević
Haris Buturović

Dragi čitaoci,

novo izdanje *FraudInfo* časopisa donosi nova razmatranja, diskurse i zanimljivosti iz oblasti prevara - *frauda* u finansijskom sektoru. Zahvaljujući pokroviteljstvu i podršci Udruženja profesionalnih rizik menadžera BiH, Fraud forum aktivno je radio i nakon izdanja prvog broja časopisa, a rezultat tog rada su, između ostalog, i stranice pred vama. UPRM ocijenio je važnom potrebu značajnijeg i konstruktivnog dijaloga na nivou finansijskog sektora o rastućem problemu prevara, što je poentirano i u prvom izdanju časopisa *FraudInfo* koji je prvi stručni časopis iz ove domene u regionu.

I u ovom izdanju nastavljamo da razgovaramo, istražujemo i dolazimo do novih spoznaja u oblasti prevara, ali i drugim srodnim oblastima i područjima rizika koji na različite načine utiču i otežavaju poslovanje u finansijskom sektoru.

Sadržaj

U ovom broju govorimo o osnovnim mjerama za prevenciju kreditnih prevara. Autori su nastojali svojim radom poentirati bazične mjere kojima se subjekti finansijskog sektora mogu zaštititi od prevara. Naime, radi se o abecedi *antifraud politike* za svakog subjekta finansijskog sektora. Dalje pišemo o mobilnom bankarstvu – segmentu poslovanja koji je nesumnjivo trend digitalnog doba kojem svjedočimo, ali istovremeno uz nove izazove prevara u ovoj oblasti. Autor ovog rada predlaže nekoliko mjera prevencije *frauda* koje *fraud* u mobilnom bankarstvu mogu svesti na najmanju moguću mjeru. Digitalno doba donosi nam nove izazove, nova sredstva komunikacije, ali i nove poslovne trendove.

Intervju sa gospodinom Muhidinom Rašidovićem, članom Tima za odgovore na računarske incidente (Vijeće ministara BiH), donosi nam niz zanimljivosti u ovom posebnom području prevara.

Posebno zanimljiva tema je i mogućnost razmjene ličnih podataka – između subjekata finansijskog sektora o počiniocima djela prevare, a o čemu vam, također, donosimo aktuelnosti u ovom izdanju. Čitaocima će biti zanimljivo pročitati i nekoliko redaka o uspostavljanju Centra za sigurnost.

Kao nastavak teksta iz prethodnog izdanja, i u ovom broju govorimo o pravnoj regulativi *frauda*, a ovaj put iz perspektive Evropske unije.

Konačno, nadamo se da i ovo izdanje *FraudInfo* časopisa doprinosi ulozi i zadaći tima autora koji se okupio oko ideje koja je izražena u ovom naslovu. Uspostavljanje nove platforme komunikacije i borbe protiv prevara u finansijskom sektoru dugoročni je cilj i Udruženja profesionalnih rizik menadžera u BiH, Fraud foruma, autora koji doprinose ovom časopisu svojom ekspertizom, ali i svih onih kojima je časopis upućen – kako bi se svijest, a tako i prevencija *frauda* u finansijskom sektoru, redovno nadograđivala. ■

UREDNIČKI TIM ČASOPISA

KREDITNE PREVARE

OSNOVNE MJERE ZA PREVENCIJU KREDITNIH PREVARA

Načini uspostavljanja i održavanja preventivnih aktivnosti i poduzimanje odgovarajućih mjera za odvraćanje potencijalnih počinilaca od pokušaja kreditnih prevara

Autori:
Eldan Dervišević
Vedran Vinšalek

Interne i ekterne kreditne prevare mogu prouzročiti značajan finansijski gubitak za banku, kao i negativan reputacijski uticaj. Kako bi se umanjio rizik od prevara, uspostavlja se opći okvir za ciklus upravljanja kreditnim prevarama koji se sastoji od četiri međusobno povezane faze prevencije, detekcije, istrage i rješavanja.

PREVENCIJA kreditnih prevara se temelji na uspostavljanju i održavanju preventivnih aktivnosti i poduzimanju odgovarajućih mjera za odvraćanje potencijalnih počinilaca od pokušaja kreditnih prevara.

Detaljna identifikacija klijenata

Primarna oblast prevencije kreditnih prevara podrazumijeva proces identifikacije klijenta. Identitet klijenta se utvrđuje u njegovom prisustvu i uvidom u službeni lični dokument koji je izdalo nadležno državno tijelo. Službeni lični dokument mora sadržavati sve nephodne zaštitne elemente.

Prilikom identifikacije potrebno je biti svjestan neobičnog **klijentovog ponašanja**. Signali kao što su agresivnost, nervoza, nesigurnost, alkoholizirano stanje, ovisnost o drogama, slabo ili nedosljedno argumentovanje svrhe kredita nas alarmiraju da izvršimo dodatne korake provjere kako bi se rizik od eventualne prevare umanjio.

> *Identitet klijenta se utvrđuje u njegovom prisustvu i uvidom u službeni lični dokument koji je izdalo nadležno državno tijelo.*

Pojedini elementi navedeni na **zahtjevu za kredit** su dobra polazna

tačka za provjeru ispravnosti podataka na kreditnom zahtjevu. Provjerom **telefonskog broja** klijenta i poslodavca u dostupnom telefonskom imeniku može biti vrlo učinkovita, jer to povećava količinu napora koji potencijalni počinitelj prevare mora uložiti. Uz navedenu mjeru kao jednu od najučinkovitijh mjera sprečavanja teških oblika kreditnih prevara je **provjera adrese**, obzirom da ista može biti jedina izravna veza uz identifikaciju klijenta, a vezana za krađu identiteta. Rizik od prevare uzrokovan manipulacijom podataka vezanih za adresu klijenta se može umanjiti tako što će se vršiti provjera adrese u vanjskim registrima, uporedbom podataka na prethodnim zahtjevima ili čak posjetom na adresu. Uvidom u dokumentaciju dostavljenu od strane klijenta potrebno je vršiti logičke provjere informacija. Treba obratiti pažnju na to da visina plaće korespondira sa stručnom spremom, godine sa radnim stažem... Provjeru **statusa uposlenja i iznosa plaće** je pored uvida u obrasce dostavljene od strane poreske uprave potrebno izvršiti tako što ćemo kontaktirati poslodavca. Treba uzeti u obzir da postoji vjerovatnoća manipulisanja kontakt podacima poslodavca pa je potrebno potražiti kontakt podatke poslodavca od strane eksternih izvora (internet, imenik itd.).

Analiza finansijskih izvještaja pravnih lica

Pored provjere gore navedenih parametara, kod klijenata pravnih lica nužno je provesti dubinsku analizu dostavljenih finansijskih izvještaja za više prethodnih godina. Pritom se treba analizirati opća slika klijenta, a ne samo propisani pokazatelji poput koeficijenata likvidnosti, zaduženosti, profitabilnosti i sl. Kako bi se utvrdila autentičnost finansijskih izvještaja, potrebno je uporediti finansijske izvještaje zaprimljene od klijenta sa finansijskim izvještajima dostupnim u AFIP/APIF-u. Provjeru finansijskih izvještaja moguće je ostvariti u poreskim bilansama i to posebno vodeći računa o podudarnosti stavki neto dobiti preduzeća u poreskim bilansama i finansijskim izvještajima klijenta.

Pregled osnovnih informacija o klijentovom zaduženju, kao i klijentovo ponašanje u otplati dugovanja

kod drugih finansijskih institucija, vidi se u **Centralnom registru kredita (CRK).** Kod klijenata kod kojih ne postoje nikakve informacije u CRK-u potrebno je obratiti posebnu pažnju, obzirom da postoji rizik od apliciranja za kredit osnovan na lažnom identitetu.

Edukacija zaposlenika

Cilj edukacije je stvoriti svijest i potrebna znanja o kreditnim prevarama. Sadržaj programa stručnog osposobljavanja i edukacije mora biti prilagođen potrebama svih uposlenika koji su u kontaktu s klijentima i ostalih uposlenika koji rade na poslovima u kojima se javlja rizik od kreditnih prevara. Sama edukacija obuhvaća upoznavanje zaposlenika s pojačanom potrebom i aktivnostima sprečavanja kreditnih prevara u svakodnevnom poslovanju te mjerama za sprečavanje kreditnih prevara.

Banke ne trebaju kriti da su bile mete prevaranata

Finansijske institucije obično nastoje od javnosti sakriti činjenicu da su bile meta prevaranata. To se može činiti opravdanim jer na taj način žele spriječiti stvaranje dojma kod klijenata da oni moraju platiti za gubitke nastale uslijed tih prevara. Međutim, moguće je poslati sasvim drukčiji signal javnosti ako se ona informira o otkrivenim prevarama. Na kraju, takve akcije imat će dvostruki pozitivan učinak: potencijalni počinitelji prevara bit će svjesni da su u određenoj finansijskoj instituciji na snazi određene procedure za sprečavanje prevara te da svaki pokušaj prevare nosi rizik od kaznenog progona. Povjerenje klijenata u sigurnost institucije će porasti nakon saznanja o pokušajima prevare koji su uspješno spriječeni.

> *Pregled osnovnih informacija o klijentovom zaduženju, kao i klijentovo ponašanje u otplati dugovanja kod drugih finansijskih institucija, vidi se u* ***Centralnom registru kredita (CRK).***

Osnivanje *Fraud foruma* kao prevencija od kreditnih prevara

Komunikacija sa drugim finansijskim institucijama uz poštivanje propisa o poslovnoj tajni i zaštiti podataka je bitan aspekt prevencije kreditnih prevara. Jedna od implementiranih mjera prevencije rizika od kreditnih pravara je osnivanje *Fraud foruma* koji ima za cilj razmjenu iskustava i jačanje saradnje između banaka u Bosni i Hercegovini kako bi se umanjili rizici od pojedinačnih i organizovanih slučajeva kreditnih prevara. ■

Upozorenje: *cyber* kriminal je u porastu

KOJE SU NAJVEĆE CYBER PRIJETNJE ZABILJEŽENE U 2017. GODINI

Banke implementiraju u višefaktorski proces autentifikacije i time pokušavaju prevenirati *cyber* napade koji su prijetnja *on line* bankarstvu

Autorica:
Sanela Stupar

Godišnji izvještaj ENISA-e ukazuje na povećanje *cyber kriminala*, a uključuje top 5 *cyber* prijetnji i trendova, a to su:

1. ***Malware*** – bilo koji dio softvera koji je napisan sa namjerom štetnog djelovanja nad podacima, uređajima ili ljudima. U 2017. godini zabilježen je porast različitih vrsta *cyber napada*, kao i različite metodologije napada i razvoja alata za napade. Proizvođači antivirusnih programa (AV) otkrivali su više od 4 miliona primjera ili 55 dnevno. U toku prvog kvartala 2017. godine zabilježeno 700 miliona primjera *malware*-a. Zanimljive karakteristike identifikovane za *malware* su da nije potrebna nikakva interakcija korisnika da bi se zarazili računari (npr. da kliknete ili otvorite zlonamjerni URL ili datoteku). Reprezentativan primjer je *WannaCry* (Wana Crypt) koja traži i šifrira 176 različitih tipova podatka i dodaje .WCRY na kraju imena i datoteke te zahtijeva od korisnika da plate otkup za *bitkoine*.

2. ***Napadi na internetu (web-based attacks)*** – Finansijski zlonamjerni softver se i dalje oslanja na *web-based* napade. Većina poznatih finansijskih *malware*-a (npr. *Zbot, Gameover Zeus, SpyEye, Ice IX, Citadel, Carberp, Bugat* i mnogi drugi) koriste eksperte pretraživača, kao što je novi nazvan *Disdain* i tehnike „čovjek u pretraživaču“ (*man-in-the-browser*).

Stručnjaci smatraju da je “čovjek u pretraživaču” najveća prijetnja *on line* bankarstvu zbog njegove efikasnosti. Zlonamjerni kod se nalazi u pretraživaču i može da modifikuje

sadržaj bankarske transakcije ili da vrši transakciju na potpuno prikriven način. Agent također sakriva transakcije od žrtava mijenjajući sadržaj u pretraživaču tehnikom ubacivanja. Važno je navesti da ni banka ni korisnik ne mogu otkriti napad. Banke su implementirale u višefaktorski proces autentifikacije koji je prevencija za navedeni napad.

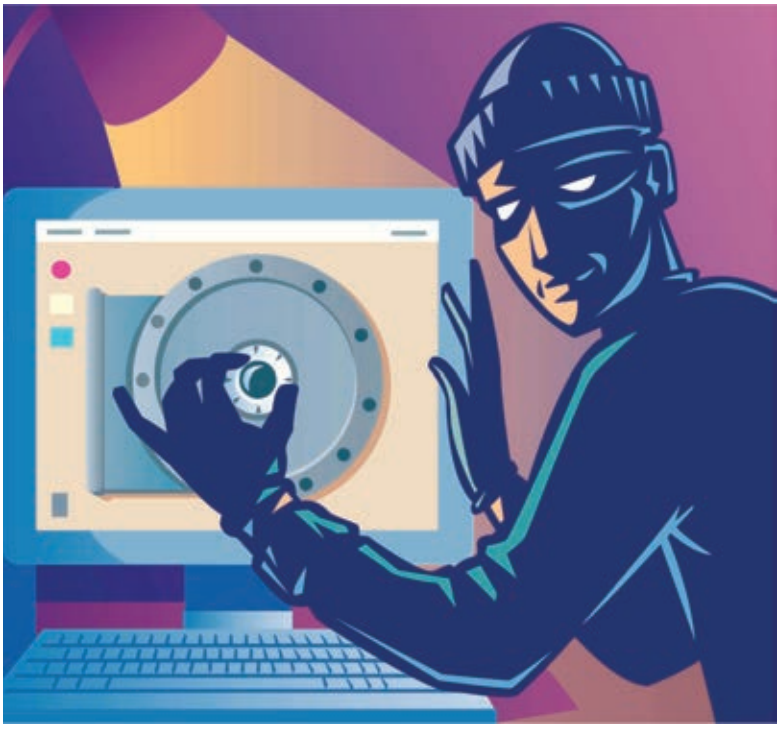
3. **Lažno predstavljanje (*phishing*)** – napad koji koristi socijalni inžinjering za napad na krajnjeg korisnika. Lažno predstavljanje se koristi kako bi se zavarali krajnji korisnici i tako zloupotrijebili osjetljivi podaci, lični podaci ili bankovni računi. U tipičnoj šemi krađe identiteta, e-poruke dovode korisnike da posjete zaražene web stranice dizajnirane za prikazivanje kao legitimne. Web stranice osmišljene su kako bi nagovorile korisnike da objavljuju finansijske podatke, kao što su bankovni računi i brojevi kreditnih kartica. Krađa identiteta obično donosi vezu ili privitak (najčešće u obliku dokumenta) koji nakon pristupa zarazi ciljni sistem zlonamjernim softverom, na primjer, zlonamjernim softverom *ransomware,* bankarski trojanski, *backdoor* itd. Preciznije, istraživanje je pokazalo da je 2017. godine 74% *cyber prijetnji* ušlo u sistem kao e-mail privitak.

4. **Neželjena pošta (*spam*)** – Neželjena pošta je jedna od najčešćih prijetnji na mreži, a postoji od početka interneta. *Spam* je i dalje ostao glavno sredstvo za isporuku zlonamjernog softvera putem zlonamjernih privitaka u pošti i zlonamjernih URL-ova. *Spam* čini više od polovice volumena e-pošte širom svijeta i uglavnom se distribuira od velikih botnet mreža. Većina neželjenih poruka jednostavno pokušava oglašavati proizvode, obično u vezi sa zdravstvenom skrbi. Unatoč smanjenju neželjenih poruka, *spam* poruke i dalje ostaju najčešće korišten kanal za *cyber kriminalce*.

5. ***Ransomware*** je oblik zlonamjernog softvera koji, nakon što ga računar preuzme, ošteti podatke i obično uskraćuje pristup vašim podacima. Napadač zahtjeva otkupninu od

žrtve, obećavajući da će vratiti pristup podacima nakon plaćanja, što često nije istina. Korisnicima se prikazuju upute za naplatu naknade za dobivanje ključa za dešifriranje. Troškovi mogu biti u rasponu od nekoliko stotina dolara do hiljadu dolara, a plaćaju se cyber kriminalcima u *bitcoinu*.

Postoji više načina na koji *ransomware* može da preuzme pristup računaru. Jedan od najčešćih sistema isporuke je lažno spamovanje – prilozi koje dolaze žrtvi u e-poštu maskirajući se kao datoteka kojoj trebaju vjerovati. Jednom kada se preuzmu i otvore, mogu preuzeti računar žrtve, posebno ako imaju ugrađene alate za socijalni inžinjering koji ometaju korisnike da dozvole administrativni pristup. Neki drugi, agresivniji oblici *ransomware*-a, kao što je *NotPetya*, iskorištavaju sigurnosne rupe kako bi zarazili računare bez potrebe da prevare korisnike. ■



Rizik od prevara putem mobilnih uređaja

FRAUD U MOBILNOM BANKARSTVU

Nesavjesnim rukovanjem pametim telefonom korisnici mobilnih uređaja postaju mete prevara

Autori:
Eldan Dervišević
Vedran Vinšalek

Prema istraživanju izvršenom od strane *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Updat*[1] predviđa se da će do 2021. godine 74,7% uređaja povezanih sa internet mrežom biti mobilni uređaji, u odnosu na 2016. godinu kada je ukupan procenat bio 36,7%.

Mi se sve više oslanjamo na mobilne telefone i mogućnosti koje oni pružaju te im povjeravamo važne informacije. Kao korisnici sada možemo da kontrolišemo svoje račune preko mobilnih uređaja koji su povezani sa internetom, da plaćamo račune te da vršimo transfere sredstava na druge banke u zemlji i izvan nje. Kao rezultat navedenog, ova pogodnost i pristupačnost otvara nova polja za *cyber kriminalce* koji mobilne uređaje posmatraju kao odličnu priliku za neovlašten pristup našim podacima i novcu. Što je nama kao korisnicima lakši pristup novcu, to je veći rizik da se navedeni kanali mogu iskoristiti za prevaru.

Kao korisnici mobilnih uređaja, moramo u svakom trenutku biti svjesni prijetnji i prevara koje nam se mogu desiti nesavjesnim rukovanjem pametim telefonom.

Metode napada cyber kriminalaca

Napadači koriste nekoliko metoda prikupljanja informacija potrebnih za izvođenje cyber napada. Jedna od metoda je tzv. **pecanje podataka ili fishing** (*phishing*) koje se zasniva na slanju poruka

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

> *Phishing se zasniva na slanju poruka putem elektronske pošte ili lažnih web stranica gdje se prevarant predstavlja kao banka i navodi korisnike na davanje povjerljivih privatnih informacija.*

putem elektronske pošte ili lažnih web stranica gdje se prevarant predstavlja kao banka i navodi korisnike na davanje povjerljivih privatnih informacija kao što su PIN elektronskih kartica, šifre za pristup mail-u, šifre za pristup uslugama elektronskog bankarstva. Jednostavniji oblik *phishinga* je kada napadač nagovara korisnika da kaže svoje podatke putem telefona gdje se napadač predstavlja kao djelatnik banke.

Druga metoda prikupljanja informacija potrebnih za izvođenje cyber napada je **korištenje softvera** (*malwere-a*) koji je dizajniran sa ciljem da prouzrokuje štetu računaru i računarskim mrežama, a u posljednje vrijeme i mobilnim uređajima. *Malware* koji je namijenjen napadima na mobilne telefone je u stalnom porastu. Tu spadaju virusi, trojanci, računarski crvi, *spyware* (špijunski programi) i bilo koji drugi programi čija je svrha da na ovaj ili onaj način ugrožavaju rad na računaru, računarske podatke i komunikaciju.

U većini slučajeva se malicioznim softverom registruju informacije koje korisnik mobilnog uređaja unese u redovnoj upotrebi te na taj način napadači mogu ukrasti osjetljive informacije uključujući lozinke za prijavljivanje, korisničke nazive, pinove i informacije o plaćanju sa mobilnih uređaja. Ove informacije se kasnije mogu koristiti za kreiranje neželjenih transakcija

putem mobilnog bankarstva. Ono što se dešava je da *cyber kriminalci* prepakuju i objavljuju zlonamjere programe koji mogu izgledati kao originalna aplikacija za mobilno bankarstvo ili bilo koja druga aplikacija preko koje pristupaju osobnim informacijama i mijenjaju funkcije telefona. Pored navedenog, krajnji korisnik može biti napadnut i putem SMS poruka.

Kako se zaštititi od napada

Od navedenih rizika možete se zaštititi poštujući određena pravila prilikom korištenja pametnih telefona. Jedno od osnovnih pravila je instaliranje aplikacija isključivo od strane provjerenih servisa (*Google play, Apple I tunes, Windows app store, BlackBerry app store...*). Jer, ako rado posežemo za besplatnim aplikacijama koje su odlične, ipak preuzimanje istih putem neoficijelnih izvora može dovesti do zaraze mobilnog telefona. Napadač bi mogao ugroziti sistem koristeći se poznatim nedostacima operativnog sistema koji nije ažuriran pa je preporučljivo redovno ažuriranje operativnog sistema, aplikacija, kao i provjerenog antivirusnog programa. Pored navedenog, potrebno je biti oprezan prilikom podešavanja sigurnosnih mobilnih postavki kako ne bi došlo do deaktivacije bitnih stavki te u svakom slučaju nipošto ne bi trebalo raditi **Jailbreak** i **ROOT** mobilnog uređaja. Vrlo jednostavan način zaštite mobilnog uređaja postiže se određivanjem PIN-a, pod uslovom da se radi o PIN-u kojeg nije jednostavno pogoditi i kojeg korisnik mobilnog uređaja drži u tajnosti.

kao i otkrivanje drugim osobama. Zasigurno najvećem riziku korisnik je izložen ukoliko nakon završetka transakcije putem usluge mobilnog bankarstva ne izvrši odjavu i ne diskonektuje sredstvo identifikacije.

> *Vrlo jednostavan način zaštite mobilnog uređaja postiže se određivanjem PIN-a, pod uslovom da se radi o PIN-u kojeg nije jednostavno pogoditi i kojeg korisnik mobilnog uređaja drži u tajnosti.*

Pravila kojih se treba pridržavati, bez obzira da li koristite pametne telefone ili računare, su oprez prilikom objavljivanja vlastitih informacija i konektovanja na nepoznate *WiFi* mreže, kao i otvaranje linkova i dokumenata dostavljenih putem e-maila od strane nepoznatih pošiljalaca. Pored navedenog je neophodno lozinke čuvati u tajnosti, izbjegavati njihovo zapisivanje, Čak je preporučljivo, u situacijama kada nije potrebno, izvršiti deaktivaciju *WiFi*-a, *Bluetooth*-a i lokacijske usluge.

Uzimajući u razmatranje naprijed navedeno, potpuna zaštita od prevara u mobilnom bankarstvu ne postoji, ali pridržavajući se naprijed navedenih pravila rizik se može svesti na minimum. ■

Zašto Bosna i Hercegovina još uvijek nema uspostavljen CERT?

CERT BIH
TIM ZA ODGOVORE NA RAČUNARSKE INCIDENTE

Nadležnosti BiH CERT-a će se isključivo odnositi na incidentne situacije gdje je uključena .ba domena ili u BiH IP adresnom prostoru

Autorica:
Sanela Stupar

Gdje možete dobiti informaciju o novim cyber napadima koji su aktuelni i na našim prostorima? Gdje možete prijaviti incident o cyber napadu? Gdje se možete informisati kako da se zaštitite od cyber napada?

Stanovnici Bosne i Hercegovine ne mogu dobiti odgovor od zvaničnih institucija u Bosni i Hercegovini na ova pitanja.

Zašto je to tako?

Dana 9.2.2005. godine Bosna i Hercegovina je potpisala *Konvenciju o cyber kriminalu* te istu ratifikovala 2006. godine. Vijeće ministara BiH je u julu 2011. godine usvojilo *Strategiju uspostave CERT-a u Bosni i Hercegovini* (CERT – Tim za odgovor na računarske incidente – Computer Emergency Response/Readiness Team), na osnovu koje

U Republici Srpskoj je Zakonom o informacionoj bezbjednosti uspostavljen CERT RS.

U Federaciji BiH nije uspostavljen CERT, a incidente možete prijaviti Federalnoj upravi policije.

Krivična djela iz oblasti kompjuterskog kriminala regulisana su entitetskim zakonodavstvom – Krivičnim zakonom Federacije BiH i Krivičnim zakonom RS-a.

je formirana radna grupa za izvršenje svih neophodnih priprema za formiranje CERT tijela na državnom nivou (BiH CERT).

Dodatno, Vijeće ministara Bosne i Hercegovine je 8.3.2017. godine donijelo *Odluku o određivanju tima za odgovor na računarske incidente za institucije Bosne i Hercegovine* u kojoj je navedeno da će „Ministarstvo sigurnosti Bosne i Hercegovine u roku **od tri mjeseca** od dana donošenja Odluke, predložiti Vijeću ministara Bosne i Hercegovine dopunu postojećeg *Pravilnika o unutrašnjoj organizaciji i sistematizaciji*, broj: 01-02-125/09 od 09.04.2009. godine, s ciljem uspostavljanja posebne unutrašnje organizacione jedinice u okviru Sektora za informatiku i telekomukacione sisteme Ministarstva sigurnosti Bosne i Hercegovine."

Ni nakon deset mjeseci od stupanja na snagu Odluke Vijeće ministara Bosne i Hercegovine prema javnim dostupnim podacima (http://www.msb.gov.ba/) Ministarstvo sigurnosti Bosne i Hercegovine nije dopunilo postojeći *Pravilnik o unutrašnjoj organizaciji i sistematizaciji*.

U Republici Srpskoj je *Zakonom o informacionoj bezbjednosti* uspostavljen CERT RS, odnosno Odjeljenje za informacionu bezbjednost. Ovo odjeljenje, kao posebna organizaciona jedinica AID RS-a, počelo je sa radom 1.6.2015. godine. Odjeljenje vrši funkciju CERT tijela RS-a. OIB - CERT RS je prvi i jedini organ ove vrste u RS i BiH. Ovo tijelo u svom radu sarađuje sa nadležnim službama MUP-a RS-a, prvenstveno sa Odjeljenjem za sprečavanje visokotehnološkog kriminala.

Iako u Federaciji BiH nije uspostavljen CERT, incidente možete prijaviti Federalnoj upravi policije koja ima Tim za istragu koji vrši istrage koristeći kompjutersku forenziku.

Krivična djela iz oblasti kompjuterskog kriminala regulisana su entitetskim zakonodavstvom – *Krivičnim zakonom Federacije Bosne i Hercegovine* i *Krivičnim zakonom Republike Srpske.*

Dijeljenje informacija je jedno od glavnih područja aktivnosti kako bi se uspostavila učinkovita upotreba CERT-a, kao što je pitanje kvaliteta i upotrebljivosti informacija, poticaj za razmjenu informacija, pravna pitanja, upozorenje za administratore informacionih resursa, kao i šire javnosti o trenutnoj informacionoj sigurnosti.

Zašto nam je potreban CERT?

Nadležnosti CERT-a propisane su aktima ENISA-e (*European Network and Information Security Agency*) i nadležnosti BiH CERT-a će se isključivo odnositi na incidentne situacije gdje je uključena **.ba** domena ili u BiH IP adresnom prostoru.

ENISA je centar za ekspertizu za cyber sigurnost. ENISA aktivno pridonosi visokoj razini mrežne i informacijske sigurnosti (network and information security – NIS) unutar Evropske Unije. Agencija blisko sarađuje s državama članicama i privatnim sektorom kako bi pružila savjete i rješenja.

U *Strategiji uspostave CERT-a u Bosni i Hercegovini*[1], navedeni su motivi za uspostavu BiH CERT-a, misija i vizija BiH CERT-a, saradnja i razmjena informacija, te obrada IT sigurnosnih incidenata.

Dijeljenje informacija je jedno od glavnih područja aktivnosti kako bi se uspostavila učinkovita upotreba CERT-a, kao što je pitanje kvaliteta i upotrebljivosti informacija, poticaj za razmjenu informacija, pravna pitanja, upozorenje za administratore informacionih resursa, kao i šire javnosti o trenutnoj informacionoj sigurnosti.

Gdje potražiti informacije o cyber sigurnosti?

Dok čekamo uspostavu CERT-a BiH, informacije možete pronaći na web portalima:

- https://cert.europa.eu – CERT – EU
- https://oib.aidrs.org/ - CERT RS – Odjeljenje za informacionu bezbjednost
- http://cert.hr/ - HR-CERT – Nacionalni CERT u Republici Hrvatskoj
- https://www.cert.si/ - SI-CERT – Slovenian Computer Emergency Response Team
- http://www.cirt.me/cirt - CERT Crna Gora

Aktivna odbrana smatra se učinkovitom strategijom koja obuhvata razne *cyber prijetnje* i koja ima za cilj ometanje kibernetičkih napada.

Preporuke kako da se zaštitite od cyber napada

Ovdje ćemo navesti samo neke osnovne korake koje trebate poduzeti u cilju sigurnosti svojih ličnih podataka i podataka na svom računaru, a to su:

- Koristite isključivo licencirane softvere.
- Instalirajte antivirus na svom računaru.
- Redovno ažurirajte operativni sistem na računaru i antivirusne programe.
- Uključite *firewall* na računaru koji koristite.
- Uvijek provjerite da li je tačan naziv internet stranice kako ne biste bili preusmjereni na lažne internet stranice u cilju prikupljanja vaših ličnih podataka (imena i prezimena, lozinke, pin za platne kartice...).
- Ne otvarajte nepoznatu poštu i priloge koje mogu imati zlonamjerne softvere.
- Vodite računa da internet oglasi mogu imati zlonamjerni softver.

Možemo naslutiti da odgovor na pitanje – ***Zašto Bosna i Hercegovina još uvijek nema uspostavljen CERT*** leži u tome da u državi ***nema političke volje,*** jer stručnjaka sigurno imamo, kako u Federaciji BiH, tako i u Republici Srpskoj. ■

[1] www.msb.gov.ba/docs/Strategija_za_CERT.doc

Borba protiv prikrivanja imovinske koristi stečene na nezakonit način

SPREČAVANJE PRANJA NOVCA

Pranje novca je globalni problem koji ima negativne efekte na socijalne, bezbjednosne i ekonomske strukture jedne zemlje

Autorica:
Ljiljana Stamenić

Pranje novca – proces prikrivanja ilegalnih izvora novca

Pranje novca (engl. *money laundering*) predstavlja proces prikrivanja ilegalnih izvora novca, tako da izgleda kao da je novac iz legalnih izvora. Naime, pranje novca je u našem zakonodavstvu normirano kao posebno krivično djelo i vezuje se u pravilu za organizovani kriminal, a često ima uporište u strukturama vlasti, tj. policiji, pravosuđu i među političarima gdje je osnovni motiv pribavljanje imovinske koristi. Radi se o veoma složenom procesu u kojem je teško identifikovati izvršioca i dokazati krivicu, s obzirom na to da su postkriminalne aktivnosti usmjerene na prikrivanje imovinske koristi stečene na nezakonit način, i to ulaganjem u finansijski i nefinansijski sistem, s ciljem da se zametne trag izvora, pri čemu je krajnji cilj njegovo ozakonjenje.

Protivpravno sticanje imovinske koristi

Valja istaći da pranje novca predstavlja nezakonito, protivpravno sticanje imovinske koristi koje se

> *Svaki novac koji je stečen iz nelagalnih izvora na jedan od navedenih načina i bez obzira na činjenicu koliko je faza, oblika ili država promijenio, odnosno da li je u konačnom reinvestiran u zakonit posao, te sva imovina koja proističe iz tako stečenog novca, sa aspekta zakona nikada neće biti legalan.*

u prvom redu generiše prometom narkotika, ilegalnom trgovinom oružja, krijumčarenjem, prevarama, utajom poreza, organizovanim kockanjem, prostitucijom, podmićivanjem, kompjuterskim prevarama i sličnim nelegalnim radnjama. Svaki novac koji je stečen iz nelagalnih izvora na jedan od navedenih načina i bez obzira na činjenicu koliko je faza, oblika ili država promijenio, odnosno da li je u konačnom reinvestiran u zakonit posao, te sva imovina koja proističe iz tako stečenog novca, sa aspekta zakona nikada neće biti legalan. Također, pranjem novca smatra se i korištenje zakonitih sredstava za nezakonite radnje kao što je finansiranje terorizma. Nadalje, ogromne sume nelegalno stečenog novca investiraju se u ekonomsku aktivnost država, a u prilog tome govori i procjena Međunarodnog monetarnog fonda, da pranje novca obuhvata 2-5% svjetskog BDP-a. Međutim, Radna grupa za finansijsku akciju (FATF) tvrdi da je nemoguće izvršiti realnu procjenu količine opranog novca jer se samo dio kriminalnih radnji otkrije. Zbog toga se i ne objavljuju statistike.

> *Radna grupa za finansijsku akciju (FATF) tvrdi da je nemoguće izvršiti realnu procjenu količine opranog novca, jer se samo dio kriminalnih radnji otkrije.*

Faze pranja novca

Iz same definicije pojma pranja novca evidentno je da se pranje novca odvija u određenom procesu, više ili manje kompleksnom, u domaćem ili međunarodnom okruženju, obuhvatajući slijed navedenih faza:

Faza polaganja (***placement***) – Ovo je najvažnija faza za detekciju, kada se sredstva, najčešće gotovina,

iz kriminalne djelatnosti ubacuju u finansijski sistem ili se pretvara u neku drugu vrstu imovine (nekretnine, umjetnine, hartije od vrijednosti, drago kamenje, itd.).

Faza raslojavanja (*layering*) – Nakon što je gotovina na neki način ušla u legalan finansijski sistem, faza raslojavanja se brojnim legitimnim transakcijama kroz tehnike promjene valuta, krijumčarenje, poslovanje preko *offshore zona*, pretvaranje novca u hartije od vrijednosti (akcije) ili pretvaranje novca u materijalnu imovinu (pokretnine, nekretnine), elektronsko prebacivanje novca, kao i falsifikovanje dokumentacije, odnosno papirnog traga novca, prikriva stvarno porijeklo tako stečenog novca.

Faza integracije (*integration*) – Obuhvata integraciju sredstava u legalnu ekonomiju i finansijski sistem u kojem je najteže detektovati čin pranja novca i samog počinitelja, s tim da se takva novčana sredstva vrlo često reinvestiraju u novi zakoniti posao.

Organizovani kriminal kao posljedica globalizacije

Globalizacija danas obično podrazumjeva rastući proces integracije nacionalnih ekonomija u jednu globalnu – svjetsku ekonomiju. Ovaj proces obuhvata proizvodnju, trgovinu, investicije i finansijske tokove, a omogućen je razvojem visokih informatičkih tehnologija. Međutim, svaki ekonomski razvoj prate i određene negativne pojave, kao što je organizovani kriminal koji nastoji da putem pranja novca legalizuje tako stečen novac, koji se zatim infiltrira u finansijske i privredne tokove. Dakle, pranje novca kao društveno negativna pojava, ne poznaje granice između država i kontinenata, a nesumnjivo ugrožava ugled, integritet i stabilnost društva, njegovih finansijskih institucija, ali i povjerenje u finansijski sistem u cjelini.

> *Pranje novca, kao društveno negativna pojava, ne poznaje granice između država i kontinenata, a nesumnjivo ugrožava ugled, integritet i stabilnost društva, njegovih finansijskih institucija, ali i povjerenje u finansijski sistem u cjelini.*

Negativni efekti pranja novca

Znači, pranje novca je globalni problem koji ima negativne efekte na socijalne, bezbjednosne i ekonomske strukture jedne zemlje. Negativni efekti pranja novca se odražavaju i na poslovanje legalnog privatnog sektora, a imaju negativan uticaj i na kretanje deviznih kurseva, smanjenje državnih prihoda i slabljenje kontrole ekonomske politike, čime se iskrivljuje struktura stvarne potrošnje, dok sredstva koja se zarađuju pranjem novca su od uticaja na porast potražnje za luksuznim proizvodima, povećanjem cijene nekretnina i nekih potrošnih dobara, a što u konačnom potiče spekulacije i inflaciju.

Borba protiv pranja novca na globalnom nivou

Kao odgovor na sve veću zabrinutost zbog pranja novca, na Samitu G-7 u Parizu 1989. godine osnovana je Radna grupa za finansijsku akciju u vezi sa pranjem novca (FATF), sa ciljem izrade politika za borbu protiv pranja novca. Tokom 2001. godine, nakon terorističkog napada na Svjetski trgovinski centar u Njujorku, ova svrha proširena je i na borbu protiv finansiranja terorizma. Inače, FATF je zadužen za proučavanje trendova pranja novca, praćenje zakonodavnih, finansijskih i policijskih aktivnosti koje se preduzimaju na nacionalnom i međunarodnom nivou, te izvještavanje o usklađenosti i izdavanje preporuka i standarda za borbu protiv pranja novca. Shodno tome, obveznici propisani *Zakonom o*

sprečavanju pranja novca i finansiranja terorističkih aktivnosti dužni su provoditi mjere za otkrivanje i sprečavanje pranja novca i finansiranja terorističkih aktivnosti. Transakcije koje se na osnovu zakona prijavljuju *Finansijsko-obavještajnom odjelu* su sumnjive transakcije, klijenti ili osobe te gotovinske transakcije i povezane gotovinske transakcije u iznosu od 30.000,00 KM i više.

U vezi s tim, postoji mnogo sofisticiranih tipologija koje se koriste za pranje novca, kao što su: falsifikovanje faktura uvoza i izvoza, razmjena novca između računa unutar banaka, putem kredita i garancija, životnog osiguranja, kupovinom luksuznih dobara, fakturisanje robe na manji iznos, avansno plaćanje za robu koja nikada nije isporučena, pozajmica, utaja poreza itd.

Kako spriječiti pranje novca

Perači stalno traže nove rute za pranje novca te su izuzetno maštoviti u stvaranju novih šema da se zaobiđu protivmjere, a najviše im pogoduju zemlje u razvoju sa slabijim mjerama zaštite, zbog čega nacionalni sistemi moraju biti dovoljno fleksibilni da bi mogli otkriti nove šeme pranja novca. Da bi borba protiv pranja novca bila bolja i efikasnija potrebno je jače angažovanje svih društvenih faktora, s ciljem da se u najvećoj mogućoj mjeri suzbije pranje novca, jer ono nesumnjivo ugrožava cjelokupan društveno-ekonomski sistem. Međutim, oblici ove organizovane kriminalne djelatnosti nisu uvijek uočljivi i prepoznatljivi i svakako otežavaju blagovremeno preduzimanje efikasnih mjera za njihovo sprečavanje i suzbijanje, tako da samo boljim i efikasnijim institucijama možemo se suprotstaviti pranju novca i time podići životni standard građana na viši nivo, i to prije svega dosljednim provođenjem zakona, ali i podizanjem društvene svijesti i efikasnijim djelovanjem represivnog aparata (policija), odnosno djelotvorim radom pravosudnih organa (tužilaštvo i sud). ■

> *„Da bi borba protiv pranja novca bila bolja i efikasnija, potrebno je jače angažovanje svih društvenih faktora, s ciljem da se u najvećoj mogućoj mjeri suzbije pranje novca jer ono nesumnjivo ugrožava cjelokupan društveno-ekonomski sistem."*

**Intervju: Muhidin Rašidović,
diplomirani kriminalist i sudski vještak za novac, dokumente i rukopise**

NE POTPISUJTE NIŠTA BJANKO!

ČAK NI KADA NEKOME OSTAVLJATE PODATKE ZA KONTAKT, NE POTPISUJTE SE!

Muhidin Rašidović, diplomirani kriminalist, jedan je od deset stalnih sudskih vještaka za novac, dokumente i rukopise u Bosni i Hercegovini. Kao ekspert u ovoj oblasti radi 15 godina te je angažovan na najsloženijim slučajevima od strane bosansko-hercegovačkih sudova svih nivoa.

Intervjuisala:
Sanela Stupar

FRAUDINFO: Kako se postaje kriminalistički vještak za ispitivanje rukopisa i dokumenata?

SV: U Bosni i Hercegovini, kao i u užem i širem okruženju, jedini način da steknete relevantna znanja iz ove oblasti je da se educirate u forenzičkim laboratorijama. Forenzičkih laboratorija, a samim tim i vještaka koji mogu pružiti ovu vrstu obuke, je veoma malo i smještene su u Ministarstvima unutrašnjih poslova ili, što je rjeđi slučaj, u razvijenim zemljama zapadne Evrope u Ministarstvima pravde. Forenzičke laboratorije su rijetke, prije svega zbog cijene opreme, potrošnog materijala i dugotrajne edukacije osoblja koje, pored osnovnog znanja stečenog na univerzitetu, mora proći dugotrajnu obuku pod mentorstvom starijih kolega. Trajanje obuke zavisi od oblasti za koju se specijalizirate, a uglavnom je to do pet godina. Obuka je strogo određena planom i programom koji je razrađen do najosnovnijih elemenata koji čine ovu oblast i situacija u kojima se može naći vještak.

FRAUDINFO: Šta mora imati jedna forenzička laboratorija za ispitivanje dokumenata i rukopisa?

SV: Osnovna oprema koju mora imati svaka prosječna forenzička laboratorija uključuje videospektralni komparator, uređaj za otkrivanje utisnutog teksta, mikroskop, lupe, razne šablone za mjerenje nagiba rukopisa i, naravno, educirano osoblje.

FRAUDINFO: Šta obuhvata posao kriminalističkog vještaka?

SV: Posao kriminalističkog vještaka za ispitivanje rukopisa i dokumenata obuhvata vještačenje rukopisa, potpisa i cifara, odnosno

svih rukom pisanih tekstova, kao i vještačenje dokumenata, raznih tekstova nastalih upotrebom pisaćih mašina, otisaka pečata i žigova. Najčešće se vještače razne vrste ugovora, priznanice, nalozi za uplatu, ali i prijeteća i oproštajna pisma.

Najteži dio posla je ispitivanje autentičnosti potpisa, jer se radi o manjem broju podataka, to jeste slova, koje izvježbani skriptor može i prekopirati pa zato vještaci rade sa spornim materijalom i materijalom za poređenje koji još zovemo i *nesporni materijal*.

Pod nespornim materijalom podrazumijevamo dvije vrste rukopisa: nesporan rukopis osobe kad nije ni znala da će joj rukopis biti vještačen, takozvani *slobodni rukopis*, a drugi je *po diktatu ili eksperimentalni*. Na taj način utvrdimo da li osumnjičeni zaista tako piše ili nešto oponaša i mijenja. Prema pravilima struke, uzimaju se rukopisi koji su vremenski bliski, naročito kada su u pitanju stariji ljudi.

FRAUDINFO: Koja je razlika između grafologije i kriminalističkog ispitivanja potpisa?

SV: Prije svega, moramo razlikovati grafologiju od kriminalističkog ispitivanja rukopisa. *Grafologija* podrazumijeva proučavanje rukopisa određene osobe i tumači karakteristike koje proizilaze iz njene psihološke strukture. Riječ *grafologija* (grč. *grapho – pišem*, i *logos – nauka)* doslovno znači da je grafologija nauka o pismu, a grafolog je osoba koja posjeduje vještinu putem koje iz rukopisa može upoznati karakterne crte osobe koja piše.

Nasuprot *grafološkog* ispitivanja koje je, prema našem mišljenju, nepouzdano i ne koristi se u dokazivanju pravnih činjenica na sudu, stoji *kriminalističko* ispitivanje rukopisa koje ima za cilj da se utvrdi porijeklo skriptora. Dakle, cilj je da se utvrdi koja osoba je potpisala ili napisala određeni dokument.

FRAUDINFO: Kako se mogu prepoznati krivotvoreni dokumenti?

SV: Svi važni dokumenti kojima se nešto dokazuje imaju manji ili veći stepen zaštite. Kada je riječ o dokumentima koje izdaje državni organ, kao što su lična karta, putne isprave te vozačke dozvole i drugi dokumenti koji se koriste u pravnom prometu, oni se štite pasivnim i aktivnim zaštitnim elementima. Pod zaštitnim elementima ovdje podrazumijevamo kvalitetne štamparske tehnike, veoma kvalitetne boje koje se koriste za štampu, poseban papir za izradu dokumenata sa velikim udjelom pamuka ili polikarbonatne podloge za izradu dokumenata nove generacije, razne optičke varijabilne elemente i sl. Da bismo mogli prepoznati krivotvoreni dokument ili novčanicu, moramo poznavati zaštitne elemente koji se nalaze na tom dokumentu ili novčanici i pravilan način kontrole. Prije svega, kada se radi na dokumentima i novčanicama koji su izrađeni na papiru, potrebno je provjeriti kvalitet papira, a to možemo uraditi i opipom ukoliko smo uvježbani, a nakon toga se treba izvršiti kontrola vodenog znaka tako što se dokument ili novčanica okrene prema izvoru svjetlosti. Kada je riječ o polikarbonatnim dokumentima, nije zgoreg dokument pogledati pod UV-lampom i provjeriti da li je došlo do destrukcije UV-zaštite u predjelu fotografije nosioca dokumenta. Kada govorimo o slabije zaštićenim dokumentima kao što su razni ugovori ili uplatnice, potrebno je utvrditi autentičnost otiska pečata i potpisa upoređujući ih sa nespornim materijalom.

> *„Najčešće se krivotvore oporuke, ugovori o kreditu, ugovori za mobilnu telefoniju, ugovori rent-a-car kompanija, potvrde o radnom stažu... U najkraćem, krivotvori se sve što može donijeti neku materijalnu korist."*

FRAUDINFO: Koji se dokumenti najviše krivotvore ili falsifikuju?

SV: To su uglavnom oporuke, ugovori o kreditu, ugovori za mobilnu telefoniju, ugovori *rent-a-car* kompanija, potvrde o radnom stažu itd. U najkraćem, krivotvori se sve što može donijeti neku materijalnu korist.

FRAUDINFO: Da li je teško krivotvoriti dokument?

SV: Sa napretkom digitalne tehnologije veoma je lako nekoga ko nije vješt ili je nedovoljno obučen u prepoznavanju krivotvorenih dokumenata dovesti u zabludu da se radi o originalnom dokumentu. Nije nikakva tajna da se uz upotrebu skenera, printera i skromnog poznavanja rada na računaru mogu dobiti prilično uvjerljivi falsifikati. Kada se tome doda i činjenica da se na pojedinim internetskim forumima mogu dobiti i detaljnija uputstva iz ove oblasti, sve postaje lakše.

FRAUDINFO: Da li je napretkom tehnologije lakše ili teže utvrditi krivotvoreni dokument?

SV: Kako napredak tehnologije pogoduje krivotvoriteljima, tako se i industrija zaštite dokumenata i novca usavršava i dolazi do novih elemenata zaštite. Rekao bih da je to stalna utrka u kojoj još nema izrazitog favorita.

FRAUDINFO: Da li imate puno predmeta za vještačenje iz bankarskog sektora (krediti, kreditne kartice i sl.)?

> *Sa napretkom digitalne tehnologije veoma je lako nekoga ko nije vješt ili je nedovoljno obučen u prepoznavanju krivotvorenih dokumenata dovesti u zabludu da se radi o originalnom dokumentu.*

SV: Do sada sam se, kao stalni sudski vještak za oblast ispitivanja dokumenata i rukopisa, susreo sa velikim brojem dokumenata, kako u parničnim sudskim sporovima, tako i u radnim sporovima. Bilo je tu raznih dokumenata, a najčešće su to zahtjevi za kredit, ostala kreditna dokumentacija, prevare u *leasingu* itd.

FRAUDINFO: Koji su bitni elementi nalaza i mišljenje vještaka?

SV: Najvažnije je utvrditi da li je vještak obezbijedio adekvatan nesporni materijal, kako u kvantitativnom, tako i u kvalitativnom smislu. Drugim riječima rečeno, potrebno je da ima dovoljan broj nespornih potpisa koji su nastali u periodu kada i sporni potpis korištenjem sličnog sredstva za pisanje i uz upotrebu istog pisma. A ovdje treba posebno istaći da u pojedinim slučajevima sporni potpis zbog svoje pojednostavljenosti ne dozvoljava stručnu analizu, jer na sebi ne posjeduje posebne karakteristike.

FRAUDINFO: Možete li izdvojiti neke interesantne slučajeve?

SV: Ne bih posebno izdvajao neke slučajeve, jer je svaki na svoj način interesantan i nijedan nije isti, a u tome je i draž ovog posla, uvijek se nešto novo pojavi. A naravno, u ovom poslu je veoma bitno čuvanje poslovne tajne klijenta koji vas angažuje.

FRAUDINFO: Koji je najbolji način da se spriječe takve pojave?

SV: Smatram da je neophodno kontinuirano obučavati osoblje koje je u direktnom kontaktu sa stanovništvom, jer su oni prva i najvažnija karika u odbrani od falsifikata. Potrebno je vršiti i redovne kontrole njihovog rada. Ukoliko je moguće, treba povećati broj izvršilaca kako bi se smanjio pritisak na radnike, ali i dati im veći vremenski okvir za kontrolu svih elemenata neophodnih za detekciju krivotvorine, bilo novčanice, potpisa ili otiska pečata.

FRAUDINFO: Koju poruku možete poslati našim čitaocima?

SV: Neophodna je stalna edukacija i upoznavanje sa najnovijim oblicima krivotvorenja, treba se maksimalno pridržavati svih radnih procedura koje su tu, prije svega, da zaštite radnika i procese unutar jednog sistema. Uvijek treba koristiti puni potpis i obavezno insistirati da se i klijenti potpisuju punim imenom i prezimenom kada god ste u mogućnosti. ■

Analiza

ODREĐENI ASPEKTI *FRAUDA* U PRAVNOJ REGULATIVI EVROPSKE UNIJE

Definicije *Frauda* u zemljama EU su različite, ali postoje minimalni uslovi koji moraju biti ispunjeni ako govorimo o *Fraudu* u finansijskim – kreditnim institucijama. Iskustvo kreditnih institucija u Uniji može bitno uticati na lokalnog zakonodavca prilikom kreiranja propisa koji bi struktuirano tretirali Fraud u kreditnim institucijama u BiH.

Autor:
Mujo Vilašević

Fraud u javnim finansijama EU

Pristup *Fraudu* u Evropskoj uniji značajno je drugačiji u odnosu na mogućnosti koje pruža važeća regulativa u Bosni i Hercegovini. U Uniji se ovo pitanje razvijalo paralelno za javni sektor, javne finansije (EU fondove) i privatni sektor, odnosno, jedinstveno finansijsko - bankarsko tržište. Pitanje *Frauda* u javnim finansijama u Uniji je aktuelno još od 1988. godine kada je formiran prvi *task force*, radna grupa Anti-Fraud Coordination Unit (UCLAF, Anti-Fraud koordinaciono tijelo) koja je koegzistirala zajedno s nacionalnim nadležnim tijelima za borbu protiv *Frauda*. Naknadno će ovo tijelo postati OLAF (francuski skraćeno za Office de Lutte Anti-Fraude, Odlukom iz 1999. godine) čija su pravila uspostavljena Uredbom 1073/1999. Danas je OLAF-u moguće prijaviti svaku sumnju na prevarno - *Fraud* postupanje u nacionalnim ili nadnacionalnim (unijskim) institucijama, a koje se tiče europskih javnih sredstava, odnosno EU fondova. Prijave je moguće izvršiti online putem (vid. v. URL: http://ec.europa.eu/anti-fraud/olaf-and-you_en), a one se potom razmatraju i poduzimaju se relevantne akcije.

Fraud u kreditnim institucijama EU

S druge strane, kada je riječ o *Fraudu* u kreditnim institucijama, ni Evropska unija donedavno nije imala jedinstven pristup. Ne smijemo zaboraviti da se radi o 28 (minus Ujedinjeno Kraljevstvo) različitih pravnih sistema i pravnih poredaka. Stoga je poznavanje EU propisa u pravilu upoznavanje 28 nacionalnih plus nadnacional-

na - unijska pravila. U segmentu *Frauda* značajan doprinos dala su istraživanja izvršena od strane EUROFINAS-a (*European Federation of Finance House Associations*, svojevrsni lokalni pandan je Udruženje banaka u BiH) i ACCIS-a (*Association of Consumer Credit Information Suppliers*, strukovno sličnom udruženju koje djeluje na teritoriji Unije), provedena naročito u toku 2011. godine. Nekoliko značajnih zaključaka proizašlo je iz ovih istraživanja. Prvo, ne postoji unijska definicija *Frauda* u kreditnim institucijama *per se*. Neke države imaju propisanu ovu definiciju, neke (poput BiH) imaju propisane definicije prevare uopće, što je primjenjivo i na kreditne institucije, a neke države uopće nemaju pravno propisanu definiciju *Frauda*. Tako npr. u Holandiji su slučajevi prevare u finansijskim uslugama definisani kao krivična djela protiv imovine koja uzrokuju pravne sankcije, u Njemačkoj je slično ponašanje definisano kao krivično djelo u Krivičnom zakonu, a u Italiji je definicija *Frauda* data kroz propise koji preuzimaju Direktivu o potrošačkim kreditima (misli se na Direktivu 2008/48/EZ o ugovorima o potrošačkim kreditima i stavljanju van snage Direktive 81/102/EEZ, OJ EU L 133/66) i koja se u najvećem dijelu bazira na krađi identiteta i lažnim činjenicama prezentiranim prilikom procjene kreditne sposobnosti (vid. v. URL: http://www.eurofi-

nas.org). Međutim, bez obzira na različitosti u definicijama *Frauda* u EU, nesporno je da su zakonodavstva i praksa iznjedrili sljedeće minimalne uslove koji moraju biti ispunjeni ako govorimo o *Fraudu* u finansijskim – kreditnim institucijama:

- ✓ oštećena strana,
- ✓ voljni akt počinioca,
- ✓ iznošenje/prezentacija zavaravajućih činjenica prilikom pregovaračke faze i stupanja u ugovorni odnos,
- ✓ namjera za postizanje ekonomske/finansijske koristi i istovremenog gubitka za drugu stranu,
- ✓ protupravna radnja.

Pomenuto istraživanje u EU iz 2011. godine pokazalo je i magnitudu uticaja *Frauda* na kreditne institucije i finansijsko poslovanje. Tako su npr. banke u Holandiji 2009. godine bilježile gubitak od 1.9 miliona EUR zbog internetskog *Frauda*, a 2010. godine 9.8 miliona EUR po istom osnovu; banke u Njemačkoj su prijavile ukupan gubitak po osnovu *Frauda* za četverogodišnji period (zaključno s 2011.) u iznosu od 255 miliona EUR; dok je u Italiji u toku 2009. i 2010. godine prijavljeno oko 25.000 slučajeva *Frauda* od strane kreditnih institucija i gubitak od cca 2 milijarde EUR. Ovi podaci naravno su nezanemarivo generisani finansijskom krizom u bliskom periodu i njenim posljedicama, no vrlo značajno pokazuju kakve posljedice *Fraud* može imati na finansijski sektor i kreditne institucije posebno, ukoliko se ovom problemu ne pristupa struktuirano. Konačno, pristup koji je ključan u borbi protiv *Frauda* je njegova prevencija. Matematički pokazano, uspjeh prevencije, detekcije, istrage i pravne reakcije proporcionalni su stepenu smanjenja *Frauda* u kreditnim institucijama.

> *U borbi protiv Frauda ključna je njegova prevencija. Uspjeh prevencije, detekcije, istrage i pravne reakcije proporcionalni su stepenu smanjenja Frauda u kreditnim institucijama.*

Sasvim sigurno, pobrojana lista dobijena istraživanjima, legislativom i značajnim iskustvom kreditnih institucija u Uniji može biti značajan faktor uticaja na lokalnog zakonodavca prilikom kreiranja propisa koji bi struktuirano tretirali *Fraud* u kreditnim institucijama u BiH.

Prevencija *Frauda* u EU

Prevencija *Frauda* i danas je (jednako kao i prethodne tri decenije) fokus Evropske unije u borbi protiv ovog tipa finansijskog kriminala. S jedne strane, tu su vrlo intezivni i struktuirani interni programi u kreditnim institucijama za prevenciju i detekciju pokušaja *Frauda* sa propisanim mitigacijskim mjerama i akcijama, a s druge su pravne mogućnosti. Pravne mogućnosti u Evropskoj uniji ulaze u sferu problema prisutnog i u Bosni i Hercegovini – zaštite ličnih podataka. Radi se o problemu koji je povezan sa tzv. listama u koje kreditne institucije unose podatke o počiniocima *Frauda*. Ove liste prisutna su praksa i u Evropskoj uniji, i to kao dvostruke: *negativna lista* – sa već identificiranim počiniocima *Frauda* i tzv. *kombinirana lista* – sa potencijalnim počiniocima *Frauda* čije su prethodne aplikacije bile pravno valjane u kreditnim institucijama, ali postoji sumnja u vezi s njihovim kredibilitetom. Pri tome su za kreditne institucije "glavobolja" povratnici u činjenju djela *Frauda* - lica koja nanovo izvršavaju takve radnje, ali u različitim kreditnim institucijama. Jasno je da bez mogućnosti razmjene podataka i pomenutih lista kreditne institucije kao entiteti za sebe nemaju pravnih mogućnosti uzajamne zaštite od *Frauda*. Pitanje zaštite ličnih podataka je u tom kontekstu vrlo značajno i otvara brojna pitanja.

"Značajna reakcija na Fraud u kreditnim institucijama Unije kroz legislativu bilo je usvajanje nove Direktive o platnim uslugama koja uvodi nove, značajno strožije zahtjeve za pokretanje i upravljanje elektronskim plaćanjima koji bi trebali da doprinesu reduciranju rizika od Frauda za sve tradicionalne mehanizme plaćanja, ali i online transakcije, kao i zaštitu povjerljivih podataka klijenata."

I pomenuto istraživanje iz 2011. godine u Uniji je dalo preporuke u ovom pravcu, odnosno, u kontekstu izmjene relevantnih unijskih propisa o zaštiti ličnih podataka. Naravno, Unija je na ove probleme reagovala.

Značajna reakcija na *Fraud* u kreditnim institucijama Unije kroz legislativu bilo je usvajanje nove Direktive o platnim uslugama (misli se na PSD 2, Direktiva EU 2015/2366 Evropskog Parlamenta i Vijeća o platnim uslugama na unutrašnjem tržištu, OJ EU L 337/35). Ova Direktiva uvodi nove, značajno strožije zahtjeve za pokretanje i upravljanje elektronskim plaćanjima koji bi trebali da doprinesu reduciranju rizika od *Frauda* za sve tradicionalne mehanizme plaćanja, ali i *online* transakcije, kao i zaštitu povjerljivih podataka klijenata. Tzv. *strong customer authentification* (SCA - stroga autentifikacija klijenta) je uvedena kao nova obaveza za pružaoce finansijskih usluga. Radi se o procesu validacije identiteta korisnika usluge, kao i validaciji željene transakcije. Ovaj proces baziran je na dva ili više elemenata definisanih kao "**ono što je poznato**" - nešto što korisnik poznaje, npr. njegova šifra ili PIN, "**ono što je u posjedu**" - nešto što korisnik posjeduje, npr. kartica i "**ono što jeste**" - nešto što je korisniku svojstveno, npr. otisak prsta ili prepoznavanje glasa, a sveukupno kako bi se validirao, autentifikovao korisnik ili transakcija. Ovi elementi su uzajamno neovisni te kršenje jednog ne uzrokuje izostanak kredibiliteta drugog, ali su dizajnirani na način da štite povjerljivost i kredibilitet datih podataka. S druge strane, i sami

korisnici su zaštićeni na način da, osim u slučaju počinjenja *Frauda* s njihove strane ili grube nepažnje, maksimalni iznos koji mogu izgubiti povodom neovlaštene transakcije na njihovim računima je 50 EUR (smanjeno u odnosu na raniju Direktivu sa 150 EUR, posebno vid. v. čl. 62-77 PSD 2). Ova Direktiva tek je otvorila proces cjelokupnom unijskom pristupu *Fraudu* kao problemu kreditnih institucija, ali sasvim sigurno dala novi okvir za postupanje. Napomene radi, države članice dužne su implementirati ovu Direktivu u njenom cilju (metodom minimalne harmonizacije) i po ocjeni vlastitih potreba mogu propisati i strožije uslove i za korisnike usluga i za kreditne institucije. Bosna i Hercegovina još uvijek nije preuzela ovu Direktivu, iako se radi o aktu koji stoji u obavezama integracije BiH.

Uredba o zaštiti ličnih podataka

S druge strane, u Evropskoj uniji se odvija i (r)evolucija propisa u oblasti zaštite ličnih podataka kroz novu Uredbu o zaštiti ličnih podataka (misli se na GDPR – *General Data Protection Regulation*, Uredba EU 2016/679 Evropskog Parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ). Nova legislativa u ovoj oblasti donosi značajne, korjenite promjene i postavlja sasvim nove obaveze za sve kontrolore i obrađivače ličnih podataka, sa izuzetno visokim sankcijama za slučaj kršenja propisanih pravila. Ova Uredba posebno daje novi uklon procjeni legitimnih interesa nosioca ličnih podataka s jedne, i interesa privatnih i javnih subjekata (kontrolora i obrađivača ličnih podataka) s druge strane. U tom smislu, pitanje *Frauda* poseban je segment ove Uredbe, o čemu će biti više govora u narednom izdanju. ■

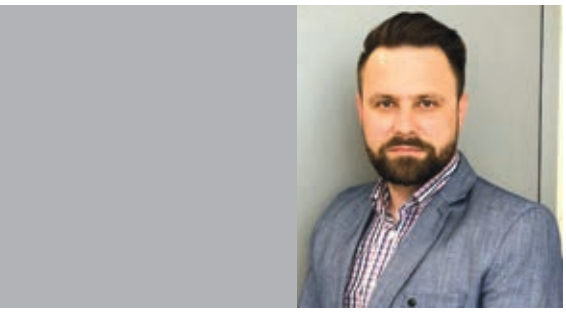
U narednom izdanju: *Fraud u novoj Uredbi EU o zaštiti ličnih podataka*

Kako se banke mogu zaštititi od prevara

MOGUĆNOST RAZMJENE LIČNIH PODATAKA

S CILJEM SPREČAVANJA PREVARNIH RADNJI

Do sada se dešavalo da jedna banka otkrije počinioca koji je istu radnju počinio kod druge banke koja bi, da je imala informaciju o počiniocu prevarnih radnji, unaprijed bila spremna izvršiti dodatne provjere podnosioca zahtjeva za korištenje bankarske usluge.



Autor:
Muris Bešić

Kao jedno od najznačajnijih pitanja koje se nametnulo u toku rada *Fraud foruma* jeste pitanje mogućnosti razmjene podataka o počiniocima prevara između banaka. Naime, ostvarivanje ideje o razmjeni podataka između banaka o počiniocima prevara je od velike važnosti zbog sprečavanja prevara u bankama. Do sada se dešavalo da jedna banka otkrije počinioca koji je istu radnju počinio kod druge banke koja bi, da je imala informaciju o počiniocu prevarnih radnji, unaprijed bila spremna izvršiti dodatne provjere podnosioca zahtjeva za korištenje bankarske usluge.

S obzirom na to da je važnost razmjene podataka o počiniocima prevara evidentna, ne treba se puno zadržavati na samom obrazlaganju svrsishodnosti razmjene podataka. Akcenat je potrebno staviti na mogućnosti navedenih postupanja u smislu primjenjivih pozitivnih propisa.

Način razmjene podataka

Kako bi se dao odgovarajući odgovor, prvenstveno je potrebno obrazložiti sam način razmjene podataka i pretpostavke koje bi banke trebale ispuniti kako bi uopšte mogle razmjenjivati podatke. Prije svega, između banaka bi trebalo usaglasiti o kojim će se slučajevima međusobno obavještavati, definisati rokove u kojima se obavijest dostavlja, kao i druge uslove saradnje povodom razmjene podataka. Imajući u vidu da je u pitanju saradnja za koju bi vrlo vjerovatno bile zainteresovane skoro sve banke, sam akt u kojem bi se propisali načini rada ne treba opterećivati formalnostima. Navedeni akt bi trebao prvenstveno sadržavati operativno-tehnička uputstva o načinu rada prilikom razmjene

Sprečavanje počinjenja krivičnih djela kroz blagovremeno informisanje zainteresovanih lica koja mogu biti žrtve prevare nesumnjivo treba posmatrati ne samo kroz zaštitu interesa samih banaka, već i kroz zaštitu javnog i općeg interesa koji se štiti putem preventivnog djelovanja.

podataka, kao i odredbe kojima se učesnice obavezuju na poštivanje propisa o zaštiti ličnih i poslovnih podataka, kao i bankarske tajne.

Postupanjem na navedeni način bi se osigurala zakonitost u radu, jer bi na taj način banke imale osnov za razmjenu ličnih podataka o počiniocima prevara. Kako bi se na adekvatan način shvatio zakonski osnov za razmjenu podataka, prvenstveno

djela kroz blagovremeno informisanje zainteresovanih lica koja mogu biti žrtve prevare nesumnjivo treba posmatrati ne samo kroz zaštitu interesa samih banaka, već i kroz zaštitu javnog i općeg interesa koji se štiti putem preventivnog djelovanja. Upravo djelovanje u cilju zaštite javnog interesa otvara mogućnost obrade podataka o počiniocima prevara u smislu člana 6. tačka d. Zakona o zaštiti ličnih podataka

Nakon usaglašavanja teksta akta koji će biti potpisan između učesnica, svakako da bi bilo korisno izvršiti konsultacije sa nadležnim državnim i entitetskim tijelima, kako je ranije navedeno, a u cilju osiguranja zakonitosti postupanja.

je potrebno konstatovati da je ova aktivnost usmjerena na sprečavanje prevarnih radnji za koje se u većini slučajeva utvrdi da postoje osnovi sumnje da predstavljaju krivično djelo, a što je u dosadašnjoj praksi u najvećem broju slučajeva potvrđeno od strane nadležnih organa. Sprečavanje počinjenja krivičnih

BiH (Sl. glasnik BiH, broj: 49/06, 76/11 i 89/11), u daljem tekstu: ZZLP, i bez saglasnosti nosilaca ličnih podataka. Dakle, čak i u slučaju da banka nema saglasnost za obradu ličnih podataka, postoji osnov za obradu istih, jer banke nesumnjivo postupaju u javnom interesu i u cilju sprečavanja počinjenja krivičnih

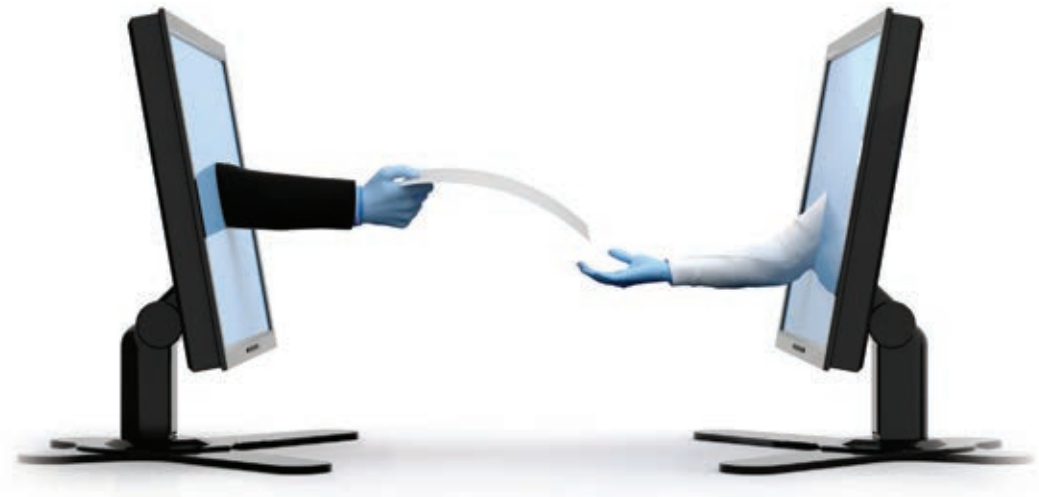
djela. Naravno, opciju obrade ličnih podataka bez saglasnosti nosilaca ličnih podataka ne treba razmatrati ukoliko banka prilikom podnošenja zahtjeva za korištenje bankarske usluge pribavi saglasnost u smislu člana 5. ZZLP, a u tom slučaju ne bi postojala prepreka za razmjenu podataka u smislu ZZLP.

Razmjena podataka treba biti u skladu sa važećim propisima BiH

Ono o čemu je također potrebno voditi računa jeste terminiologija koja se koristi prilikom razmjene podataka i sačinjavanja platforme putem koje se će se vršiti razmjena podataka o prevarnim radnjama. Naime, imajući u vidu pretpostavku nevinosti koja je propisana krivičnim propisima te da se postojanje krivičnog djela isključivo može utvrditi u zakonom propisanom postupku koji je vođen pred nadležnim sudom i na osnovu pravosnažne presude, banke bi prilikom razmjene podataka isključivo trebale vršiti razmjenu podataka o činjenicama. Razmjena podataka o činjenicama i ličnim podacima eventualnih počinilaca prevara predstavlja sasvim dovoljno informacija da bi se druge banke uputile na povećan oprez prilikom uspostave poslovnog odnosa sa određenim

licem. Komunikacija podataka ni u kojem slučaju ne smije značiti da je bilo kojoj banci zabranjeno uspostavljanje poslovnog odnosa sa određenim licem. Donošenje odluke o uspostavi poslovnog odnosa je u isključivoj nadležnosti svake od banaka i u skladu sa njenim internim organizacionim pravilima.

Ne treba zanemariti činjenicu da je ova ideja u samom začetku te je svakako preporučljivo da se prije njene realizacije obave konsultacije ili pribavi mišljenje nadležnih tijela koja se bave nadzorom nad primjenom propisa o zaštiti ličnih podataka, a po potrebi i sa tijelima koja se bave nadzorom nad primjenom propisa kojima se štiti bankarska i poslovna tajna. Mada, u suštini, ukoliko se prilikom podnošenje zahtjeva za korištenje bankarske usluge pribavi saglasnost nosioca ličnih podataka, bez sumnje se može reći da banka ima osnov za otkrivanje bankarske tajne u smislu člana 104. Zakona o bankama FBiH (Sl. novine FBiH 27/17) i člana 128. Zakona o bankama RS (Sl. glasnik RS 3/16).



Kako se ne bi zadržali samo na osmišljavanju načina rada i pretpostavkama koje je potrebno ispuniti da bi se osiguralo zakonito postupanje, potrebno je u cilju cjelovite obrade teme predložiti i korake koje bi banke trebale poduzeti u cilju ostvarenja predmetne zamisli.

Prvenstveno je potrebno osmisliti izgled i sadržaj same platforme putem koje bi se vršila razmjena podataka, putem posebnih mail adresa ili na neki drugi način. Nakon navedenog, banke bi trebale pristupiti usaglašavanju teksta Protokola o saradnji u kojem bi se precizirala prava i obaveze svih učesnica, kao i propisao sam način rada povodom razmjene podataka. S obzirom na to da je ovakav način rada u samom začetku, nakon usaglašavanja teksta akta koji će biti potpisan između učesnica, svakako da bi bilo korisno izvršiti konsultacije sa nadležnim državnim i entitetskim tijelima, kako je ranije navedeno, a u cilju osiguranja zakonitosti postupanja.

U svakom slučaju, prilikom implementacije ovog načina rada potrebno je prvenstveno imati u vidu koristi koje nosi sa sobom te se ne zadržavati na restriktivnim formalističkim pristupima koji bi mogli onemogućiti ostvarenje navedene ideje jer se na taj način direktno pogoduje počiniocima prevara, a u konačnici se bankarski sektor u BiH kao i društvo u cjelini izlaže rizicima od počinjenja krivičnih djela. ■

U narednom izdanju: *Osiguranje od rizika prevara i drugih rizika*

Jedini neriješeni slučaj vazdušne piraterije u historiji putničkog vazduhoplovstva SAD-a

NEPOZNATI PLJAČKAŠ S ARMIJOM SLJEDBENIKA

Izvjesni D.B. Kuper je prije skoro pola vijeka oteo avion i s dobijenim novcem iskočio padobranom.

Nikada ga nisu uhvatili...

Autor:
Tanasije Sofrenović

Imenom **D.B. Kuper** američki Federalni istražni biro (FBI) označio je nepoznatog muškarca koji je 24. novembra 1971. godine oteo avion *boing 727* na liniji Portland – Sijetl. U pilotskoj kabini uspio je da stupi u vezu sa FBI-em, zaprijetivši da će dići avion u vazduh ako mu se, po slijetanju u Sijetl, ne isplati 200.000 dolara (današnjih 1,2 miliona) i ne donese padobran. Vlasti su pristale, jer je stjuardesa potvrdila da otmičar ima razorni eksploziv. Isplaćen mu je novac, a Kuper je pustio putnike i avion se ponovo vinuo u vazduh. Nakon pola sata leta otmičar je

iskočio i time je počela najopsežnija potjera za opljačkanim blagom i dugotrajno istraživanje jedinog neriješenog slučaja vazdušne piraterije u historiji putničkog vazduhoplovstva SAD-a.

Četrdeset šest godina nakon otmice, uprkos 60 tomova istražnih spisa, nema konačnih zaključaka šta se zapravo dogodilo sa Kuperom, ko je zapravo on i gdje se krije. Na početku istrage stručnjaci su rekli kako najvjerovatnije nije preživio ovaj rizični skok, ali njegovo tijelo nikada nije nađeno. Zna se da je avionsku kartu kupio pod lažnim imenom Den Kuper, ali je, pošto su mediji o njemu brujali ispredajući čitave pripovijesti, postao poznat kao D.B. Kuper. Do februara 1980. godine slučaj nije privlačio veliku pažnju javnosti. Tada su na obali rijeke Kolumbije nađene prilično oštećene novčanice ukupne vrijednosti 5.000 dolara. Za njih je pouzdano utvrđeno da su isplaćene otmičaru *boinga* devet godina ranije. Ovo otkriće samo je produbilo misteriju. Legenda o D.B. Kuperu je rođena, o njoj se piše svakodnevno, a odluka FBI-a iz jula 2016. godine da okonča istragu dovela je do novih nagađanja.

Svako plaća svoje piće

Šta su tokom opsežne istrage otkrili detektivi? Tog novembra, čovjek sa crnom tašnom približio se šalteru prevoznika *Nortistern* na međunarodnom aerodromu u Portlandu. Predstavivši se kao Den Kuper, kupio je kartu u jednom pravcu do Sijetla. Smjestio se u zadnjem dijelu prostora za putnike, zapalio cigaretu i naručio burbon sa sodom. Očevici su ga opisali kao čovjeka četrdesetih godina, visokog oko 1,80 m, a nosio je laganu crnu kabanicu, mokasine, bijelu košulju i crnu kravatu. Stjuardesi Florens Šafner zapala je za oko njegova sedefna igla za kravatu. Kada je avion poletio, Kuper ju je pozvao i šapatom joj, otvarajući tašnu na susjednom sjedištu, rekao: – „Gospođice, pogledajte, imam bombu". Razrogačenih očiju, bez daha, Florens je buljila u osam cilindričnih predmeta presvučenih crvenom izolir-trakom, vezanih za baterije. Hladnim glasom naredio joj je da o tome obavijesti pilota i vlastima u Sijetlu prenese da mu spreme 200.000 dolara i četiri padobrana, dva glavna i dva pomoćna. Također, na pisti mora da bude cisterna sa gorivom, jer avion nastavlja put. Pilot je postupio po uputstvima otmičara. Predsjednik aviokompanije, Donald Nirop, naredio je svim zaposlenima potpunu saradnju sa otmičarem.

„Nije bio nervozan", rekla je docnije Florens Šafner istražiteljima. „Izgledao je prilično hladnokrvno, smiren i ljubazan sve vrijeme. Popio je još jedan burbon i platio ga prije nego što smo napustili avion".

Iznad aerodroma u Sijetlu avion je kružio oko dva sata kako bi se omogućilo da policija i FBI sakupe novac i nabave padobrane. U 5.24 h poslije podne stjuardesa Šafner obavijestila je otmičara da su svi njegovi uslovi ispunjeni. Avion je sletio u 5.39 h, obavljena je razmjena, u avion je natočeno gorivo, putnici i stjuardese mirno su izašli iz aviona. „Nije bio nervozan“, rekla je docnije Florens Šafner istražiteljima, „izgledao je prilično hladnokrvno, smiren i ljubazan sve vrijeme. Popio je još jedan burbon i platio ga prije nego što smo napustili avion“.

Tokom punjenja rezervoara Kuper je pilotima iznio plan leta. Pistom su zarulali oko 7.40 h na putu za Rino, a oko 8.13 h Kuper je, sa torbom novca zakačenom za pojas i crnom aktovkom u ruci, iskočio iz aviona iznad južnog oboda planine Sveta Jelena u oblasti rijeke Luis, u blizini vještačkog jezera Mervin, jugozapadno od Vašingtona.

Kada je *boing* sletio u Rino, policija je opkolila avion i detaljno ga pretražila misleći da se otmičar negdje pritajio. Nisu vjerovali da se odvažio na krajnje opasan skok. Agenti i policija okruga Klark i Koulic, oblasti gdje je Kuper iskočio, odmah su helikopterima i sa psima, uz pomoć vatrogasaca i dobrovoljaca, krenuli u *češljanje* terena prekrivenog gustom crnogoričnom šumom. Duž obale rijeke Luis i jezera Marvin poslano je desetak patrolnih brodova. Višednevna pretraga nije urodila plodom, od padobranca ni traga ni glasa.

Novac u pijesku

Jedan od glavnih istražitelja FBI-a, iskusni Džeri Tomas, kasnije je rekao da procjena gdje će Kuper sletjeti nije bila dobra. U obzir nije uzet izuzetno snažan vjetar koji je duvao te večeri. On je padobranca odnio više od 100 km na jugoistok od prvobitne procjene, čak u oblast sliva rijeke Vašugal. Narednih mjeseci dolinu rijeke i okolinu

dodatno su preteresali, ali bez rezultata.

Krajem 1971. godine FBI šalje listu serijskih brojeva sa iznuđenih novčanica svim finansijskim ustanovama, očekujući da se novčanice ipak negdje pojave, u nekoj samoposluzi, hotelu, bilo kojoj prodavnici. Avioprevoznik je ponudio nagradu u iznosu od 15 procenata otetog novca (danas oko 180.000 dolara) onome ko ih navede na pravi trag. FBI je ponudio 25.000 dolara. U ponudama im se pridružuje i tabloidna štampa Oregona nudeći nagrade između hiljadu i pet hiljada dolara.

Godine 1976. država se konačno odlučuje da podigne optužnicu protiv „osobe u odsustvu" Dena Kupera, zvanog D.B. Kuper, zbog piraterije i kršenja zakona. Optužnica zvanično upućuje kako gonjenje otmičara može da se nastavi „ne bi li se Kuper uhvatio u bilo kom trenutku u budućnosti". FBI je marljivo nastavio da traga za njim godinama sakupljajući sve moguće dokaze.

Tako je 1978. godine lovac na jelene na 21 km od Kasl Roka (Vašington) našao uputstvo o otvaranju zadnjih vrata na *boingu 727* istrgnuto iz avionskog priručnika. Dvije godine kasnije Brajan Ingram bio je na odmoru sa porodicom na obali rijeke Kolumbija, 14 km nizvodno od gradića Vankuver (Vašington). Spremao se da na pješačkoj plaži raspali roštilj. Dubeći rupu u pijesku gdje će staviti brikete, iskopao je paket uvezan gumenim trakama. Kada ga je otvorio, našao je svežnjeve vlažnih, gotovo raspadnutih novčanica od dvadeset dolara.

Tehničar FBI-a potvrdio je da je novac, ukupno 5.000 dolara, bio dio otkupnine isplaćene Kuperu kako ne bi avion sa 42 putnika i članova posade digao u vazduh. Ovo otkriće potvrdilo je saznanje kako otmičar nije sletio u blizini jezera Mervin, niti u bilo koju drugu oblast rijeke Luis. Zašto se uopšte tu zaustavio i zakopao paket, ostala je tajna. Cijeli teren pretražen je da bi se još nešto našlo, padobran na primjer.

Ispitivanja su djelomično urodila plodom, jer je u obližnjem šumarku nađena njegova kravata. Ona je podvrgnuta podrobnom ispitivanju pomoću mikroskopa i moderne tehnologije. Novembra 2011. godine na njoj su nađene čestice čistog titaniuma, cezijuma i stroncijum-sulfida. To je istražitelje navelo da je D.B. Kuper možda bio hemičar, metalurg, zaposlen u nekoj od *Boingovih* fabrika. To nije mnogo pomoglo i potraga je nastavljena.

Krajem aprila 2013. godine policija je otkrila skriveni padobran ispitujući pripadnike padobranske škole iz Vudenvila, predgrađa Sijetla. Vještačenjem je utvrđeno da je baš taj padobran iskoristio Kuper. Na pitanje kako se tu našao i ko ga je uspješno krio pune 43 godine nije bilo odgovora.

Osumnjičeni

Tokom dalje istrage FBI je osumnjičio preko 1.000 lica usredsređujući se na nekoliko mogućih D. B. Kupera. Dugo je prvi na listi bio **Teodor D. Mejfild**, iskusni pripadnik specijalnih jedinica i padobranski instruktor. Godine 1994. optužen je za ubistvo iz nehata, pošto su dva njegova učenika poginula kada im se padobrani nisu otvorili zbog neispravne opreme. Kasnije je utvrđeno da je odgovoran za smrt još 13 padobranaca zbog loše obuke. Godine 2010. dopao je robije zbog oružane pljačke i prevoza ukradenih aviona sa raznih aerodoroma.

Ričard Flojd Makoj, vojni veteran, bio je dvije godine u Vijetnamu kao stručnjak za miniranje, potom je u *zelenim beretkama* vozio helikopter. Nakon rata postao je oficir Nacionalne garde države Juta i strastveni rekreativni padobranac. On je 7. aprila 1972. godine oteo *boing 727* na letu San Francisko – Denver tražeći padobrane i pola miliona dolara (današnja vrijednost 2,8 miliona). Prilikom uručenja novca u San Francisku uhvaćen je i osuđen na 45 godina robije. Iz zatvora je uspio da pobjegne u kamionu za

smeće. Tri mjeseca kasnije ubijen je u Virdžinija Biču nakon razmjene vatre s policijom. Tokom prethodne istrage pobio je sve optužbe da je on zapravo D. B. Kuper, samo je otmicu pokušao da izvede u njegovom stilu.

U knjizi *D. B. Kuper je Makoj*, objavljenoj 1991. godine, novinar Berni Rouds i agent FBI-a Rasel Kalami navode očigledne sličnosti u obje avionske otmice i vrhunsku obučenost otmičara, ali ranija istraga nesumnjivo je utvrdila da je Makoj, onoga dana kada je otet avion na letu za Sijetl, bio na večeri sa porodicom, što su potvrdili svi njeni tada prisutni mnogobrojni članovi.

Naredno ime na FBI listi osumnjičenih bio je **Robert Rokstro**, penzionisani vojni pilot helikoptera tokom rata u Vijetnamu i bivši zatvorenik. Robijao je zbog krivotvorenja savezne pilotske dozvole. Pošto nije bilo neposrednih dokaza protiv njega, oslobođen je svake sumnje.

„Podvig D. B. Kupera nadahnuo je nalet imitatora, najviše tokom 1972. godine kada su pokušane čak 32 avionske otmice u SAD-u. To je ubrzalo izmjene zakonskih propisa i uvođenje stroge provjere putnika i prtljaga u prevozu. **Garet Brok Trapnel** oteo je avion preduzeća TVA na putu od Los Anđelesa do Londona, tražeći oslobađanje političke zatvorenice Anđele Dejvis i 306.800 dolara u gotovini. Po slijetanju aviona na aerodrom *Kenedi* Trapnel je ranjen, a potom i uhapšen.

Ričardu Čarlsu Lapointu pošlo je za rukom da otme avion prije polijetanja na aerodoromu u Los Anđelesu slijedeći *Kuperov obrazac*. Prijetnja bombom je uspjela, FBI mu je dao 50.000 dolara i dva padobrana. Avion *DC-9* uzeo je kurs ka Koloradu gdje je Lapoint iskočio nad njegovim pustinjskim sjeveroistočnim dijelom. Uspješno se prizemljio i kada je pomislio da je uspio, bio je uhapšen dva sata kasnije. FBI je u torbu sa novcem i u padobransku opremu stavio radiolokatore. Oni su agente lako doveli do lopova.

U aprilu iste godine bivši oficir *zelenih beretki* **Ričard Makoj mlađi** oteo je avion *Junajted Erlajnza* nakon što je ovaj uzletio iz Denvera ka San Francisku. Sve je uradio kao i misteriozni D. B. Kuper, iskočivši sa pola miliona dolara negdje iznad Jute. Dva dana se krio u usamljenoj šumskoj kolibi, opremljenoj hranom i vodom za mjesec dana, kada su mu agenti FBI-a dvije večeri kasnije zakucali na vrata. I ovaj put ubacivanje lokatora bilo je presudno za uspješno okončavanje operacije.

Frederik Hejneman bio je maštovitiji. Sve je uradio po proslavljenom receptu vazdušne piraterije, ali je iskočio iznad prašume Hondurasa, svoje rodne zemlje, sa 303.000 dolara. FBI ga je ucijenio sa 25.000 dolara i poslije mjesec dana Hajneman se predao američkoj ambasadi u Tegusigalpi. Nije stigao da potroši ni hiljadu dolara. Prilikom predaje je rekao: "Otkad je vlada SAD-a objavila potjernicu, na mene je pucano tri puta, a dva puta me umalo nisu uhvatili lovci na glave. Nisam imao mira, život mi je visio o koncu pa mi je bilo najsigurnije da se predam i vratim novac".

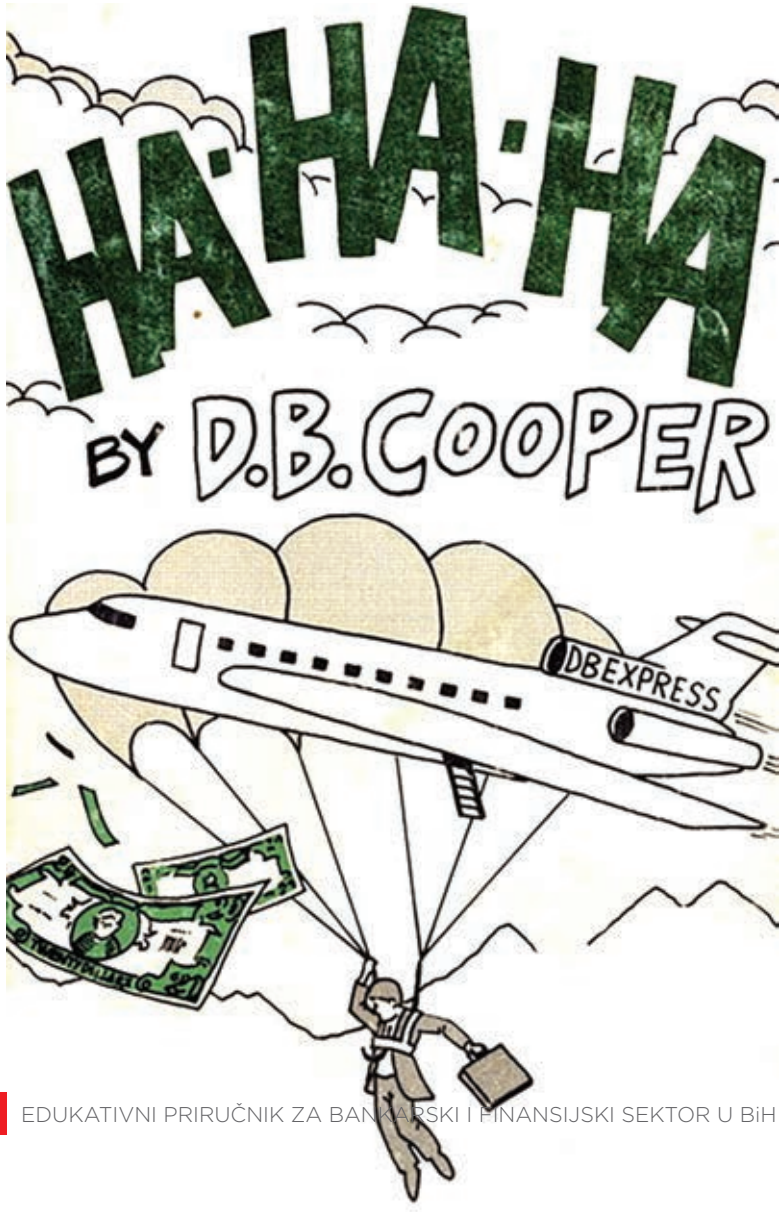
Zvijezda je rođena

Još jedan profesionalni padobranac i vijetnamski veteran, **Rob Dolin Hidi**, uspješno je iskoristio *recepturu* D. B. Kupera. Sa 200.000 dolara iskočio je u mrak blizu jezera Vašo, 40 km južno od Rina. Policija je našla njegov automobil parkiran kraj jezera i sutradan ga uhapsila kada je došao po njega noseći vreću sa novcem.

Martin Maknali, nezaposleni stjuard, također je sve uradio kao D.B. Kuper, ali mu se vreća sa pola miliona dolara otkačila prilikom skoka. Novac je brzo nađen zahvaljujući radiolokatoru, a malerozni Martin dopao je u ruke zakona nekoliko dana kasnije u predgrađu Detroita dok je u kafiću ispijao prvu jutarnju kafu. Sve u svemu, tokom 1972. godine ukupno je pokušano 15 otmica *a-la-Kuper* i sve su završile neuspješno.

Nedavno je TV kanal *Histori* (History Channel) prikazao trodijelnu seriju pod nazivom *D.B. Kuper, slučaj zatvoren*. Autor Den Rej vjeruje da se iza ovog pseudonima krije Robert Rokstro, veteran rata u Vijetnamu, član elitne Prve konjičke (tenkovske) divizije. Od običnog reda tokom karijere napredovao je do poručnika. On je označen kao mogući počinilac 1978. godine „jer je, služeći vojni rok prije Vijetnamskog rata i tokom njega, uradio niz nezamislivih stvari".

Godine 1979. Rokstro je dao intervju Vorenu Olniju, reporteru mreže *KNBC*, negirajući da je otmičar, jer se boji visine. Međutim, istraživanje Dena Reja otkriva da je ovaj svojevremeno uspješno pohađao vojnu padobransku školu u bazi *Fort Bening* u Džordžiji, gdje je njegova vještina ocijenjena najvišim ocjenama, a zbog izuzetnih uspjeha u vojnoj službi, dobio je vazduhoplovnu Srebrenu zvijezdu. Odmah nakon položenog padobranskog ispita, prošao je i obuku za pilota helikoptera. Upoređujući fotorobot D. B. Kupera i fotografije Rokstroa iz tog vremena, producenti dokumentarca ustanovili su zapanjujuću sličnost.



Kada su avionskom osoblju i putnicima otetog aviona pokazivali njegovu fotografiju, svi su, osim stjuardese Florens Šafran sa kojom je najviše razgovarao, potvrdili da je to on. Florens ga nije prepoznala kao D.B. Kupera, jer je, kako tvrde FBI istražitelji, uslijed traumatičnog iskustva, trajno izgubila sjećanje na taj dogadjaj.

Den Rej je snimajući dokumentarac više puta pokušao da razgovara sa sedamdesetdvogodišnjim Robertom Rokstroom, ali je on svaki razgovor odlučno odbio ponavljajući da su sve optužbe protiv njega odbačene prije 38 godina. Danas je misteriozni D. B. Kuper, vazdušni pirat i iznuđivač, neka vrsta pop-ikone u američkoj kulturi. Na aerodromima se prodaju suveniri s njegovim likom, a u gradiću Arijelu, nedaleko od Vašingtona, svetkuje se Kuperov dan u restoranima i kuglanama. Njegov lik i djelo opisani su u brojnim pripovijetkama, a najveću slavu doživio je u TV-serijama *Bjekstvo iz zatvora* i *4400*. ■

UREDNIČKI TIM

Muris Bešić
Voditelj odjela za pravnu podršku mreži - Direkcija pravnih poslova u Sparkasse Bank d.d. BiH

Haris Buturović
Direktor direkcije operativnih rizika i informacijske sigurnosti u Sparkasse Bank d.d. BiH

Eldan Dervišević
Voditelj funkcije sprečavanja kreditnih prevara u UniCredit Bank d.d. Mostar

Ina Hasanbegović
Compliance Officer & Fraud Specialist u Raiffeisen Bank d.d. BiH

Tanasije Sofrenović
Ovlašteni revizor / Stručni saradnik u Udruženju profesionalnih rizik menadžera u BiH

Ljiljana Stamenić
Viši saradnik za usklađenost i sprečavanje pranja novca u Sberbank a.d. Banja Luka

Sanela Stupar
Voditelj Odjela za usklađenost i SPNiFT NLB Banke d.d. Sarajevo

Mujo Vilašević
Samostalni stručni saradnik za usklađenost u Sparkasse Bank d.d. BiH

Vedran Vinšalek
Samostalni stručni saradnik za upravljanje rizikom finansijskog kriminala u Sparkasse Bank d.d. BiH

EUROPEAN FUND FOR SOUTHEAST EUROPE
DEVELOPMENT FACILITY

THE EFSE DEVELOPMENT FACILITY

A RELIABLE PARTNER IN CHALLENGING TIMES

The Development Facility of the European Fund for Southeast Europe (EFSE DF) was created in 2006 to support the fund's development finance mandate.

The EFSE DF deploys effective, targeted and innovative technical assistance to maximise the impact and extent of the fund's activities in target countries. The facility's services strengthen the internal capacities and operations of the fund's partner lending institutions through:

- ✓ **Capacity building**
- ✓ **Training**
- ✓ **Mentorship**
- ✓ **Applied research**
- ✓ **Financial sector support**

For more information, please contact **ta@finance-in-motion.com** or visit **www.efse.lu**