Primljeno: srpanj 2019.

DAMIR BILIĆ*

# Zloporaba platnih kartica

***Sažetak***

*Kriminal u području zloporabe i falsificiranja platnih kartica novijeg je datuma kod nas, ali se može reći da je sve zastupljeniji. Kao i gotov novac, platne kartice mogu biti predmet kaznenog djela krađe, pronevjere ili nekog drugog kaznenog djela protiv imovine (teške krađe, razbojništva, razbojničke krađe, prijevare i slično). Globalna rasprostranjenost platnih kartica, njihova jednostavnost uporabe i laka dostupnost modernih tehnologija, učinile su ove kartice izuzetno primamljivim objektom napada kriminalaca, ali i organiziranih kriminalnih skupina.*

***Ključne riječi:*** *platne kartice, bankomat, krađa, skiming, pecanje, elektroničko bankarstvo, elektronički ili digitalni novac.*

## 1. UVOD

U Bosni i Hercegovini, kriminal u području zloporabe i falsificiranja platnih kartica novijeg je datuma i moglo bi se reći da je sve zastupljeniji. S više aspekata može se promatrati ovakav oblik kriminala koji predstavlja jedan suvremeniji i noviji oblik kriminala, i to s aspekta činjenja ovog kriminala, specifičnosti osoba koje mogu biti počinitelji, sredstava počinjenja, mjesta i vremena počinjenja, kriminalnih djelatnosti i specifičnosti nastalih posljedica. Ove promjene stvorile su društvo koje je bazirano na znanosti, znanju, informacijama, inovacijama, intelektualnoj svojini i praktičnoj primjeni visokih tehnologija koje su omogućile neusporedivo brži protok robe i usluga.[1]

U razvoju bankarstva najveće dostignuće informacijskih tehnologija pojava je elektroničkog novca. Elektronički je novac specifična monetarna informacija koja se putem elek-

* Damir Bilić, Pravni fakultet Univerziteta u Travniku; student postdiplomskog studija.

[1] Đokić, Z. (2008), Falsifikovanje i zloupotrebe platnih kartica, zbornik radova, Internacionalna asocijacija kriminalista, Brčko, str. 482.

tronskih impulsa u realnom vremenu prenosi između transaktera koji obavljaju plaćanje[2], ili, u širem smislu, elektronički ili digitalni novac može se definirati kao novac koji se kreće kroz elektroničke medije, odnosno izvan uobičajenih kanala plaćanja koje tradicionalno podržavaju banke.[3]

Promatrajući kriminal kao dinamičnu i izrazito prilagodljivu društveno negativnu pojavu, može se konstatirati da kriminal ima svoju prošlost, sadašnjost ali i viziju razvoja u budućnosti što ovisi o ukupnim društvenim okolnostima (ekonomskim, političkim, moralnim, pravnim) te organiziranosti; te profesionalne i stručne spremnosti nadležnih subjekata da mu se suprotstave, s jedne druge strane. ATM uređaj, odnosno bankomat[4], kao suvremeno tehničko sredstvo, zajedno s platnim karticama, nije mogao ostati izvan sfere kriminala.[5]

## 2. ZLOPORABA PLATNIH KARTICA

Platna je kartica suvremeni instrument bezgotovinskog plaćanja koji obavlja tri funkcije, i to[6]: sredstvo bezgotovinskog platnog prometa, instrument kreditiranja korisnika i općeprihvaćeno internacionalno i nacionalno sredstvo plaćanja. Platna kartica predstavlja jednu vrstu isprave kojom se vlasnik opunomoćuje za bezgotovinsko plaćanje, također, predstavlja i vrstu rasprostranjenog bezgotovinskog načina plaćanja roba i usluga trgovcima[7], ili se rabi za podizanje novca na bankomatima.

Globalna rasprostranjenost platnih kartica, njihova jednostavnost korištenja i laka dostupnost modernih tehnologija, učinile su ove kartice izuzetno primamljivim objektom napada kriminalaca ali i organiziranih kriminalnih skupina. Na meti su kriminalaca nova i nedovoljno razvijena tržišta, bez dovoljno iskustava i u kojima ne postoji sustav za prepoznavanje i sprječavanje zloporaba. Uvođenje platnih kartica s čipom postalo je obvezni standard zaštite platnih kartica na području zemalja Europske unije. Međutim, to nosi realnu opasnost od migracije kriminala ka tržištu zemalja koje još nisu uvele čip-tehnologiju. Na primjer, 2009. godine nastupila je migracija kriminala kojim se čini zloporaba i falsificiranje platnih kartica na prostorima zemalja jugoistočne Europe gdje se lažne kartice zlorabe na bankomatima.

Razvoj je kartičarstva na naše prostore donio i kriminal zloporabe platnih kartica.

Prvi razlog porasta broja počinjenih kaznenih djela, već smo spomenuli, jest migracija ove vrste kriminala iz zemalja Europske unije. Drugi je razlog povećanje broja platnih kartica i akceptorske mreže. Ovisno o tome tko je počinitelj prijevare, gdje i kako se zloporabe realiziraju, prijevare s platnim karticama, mogu se podijeliti u određene kategorije.

---

[2] Vasković, V. (2007), Sistemi plaćanja u elektronskom poslovanju, Fakultet organizacionih nauka, Beograd, str. 48

[3] Zečević, M. (2009), Bankarstvo, Evropski Univerzitet Beograd, Beograd, str. 536.

[4] Bankomat – Automated Teller Machine (ATM) predstavlja samouslužni automatski aparat za podizanje gotovine, provjeru stanja na računu i druge šalterske usluge.

[5] Zečević, M. (2009), Bankarstvo, Evropski Univerzitet Beograd, Beograd, str. 305.

[6] Pena, U. i Pantić, S. (2019), Falsifikovanje i zloupotreba platnih kartica, Zavod za udžbenike i nastavna sredstva, Istočno Novo Sarajevo, str. 30.

[7] Trgovcem se smatra svako prodajno mjesto koje posjeduje POS terminal, ili je registrirano za internetska plaćanja.

Razlikuju se zloporabe korisnika kartica, prijevare akceptora, prijevare s falsificiranim karticama i prijevare za čije počinjenje nije potrebna kartica u fizičkom obliku. Pretpostavka za uspješno suprotstavljanje ovim kaznenim djelima jest poznavanje pojavnih oblika i načina počinjenja falsificiranja i zloporabe platnih kartica. Osnovni pojavni oblici ovog kaznenog djela su sljedeći:

- zloporaba ukradenih ili izgubljenih platnih kartica
- neovlaštena uporaba tuđe platne kartice
- zloporaba neuručenih platnih kartica
- zloporabe i prijevare koje počine akceptanti - trgovci
- pribavljanje podataka za izradu lažne platne kartice
- izrada i zloporaba lažnih platnih kartica
- zloporaba koju počine korisnici i
- računalne prijevare i zloporabe platnih kartica.

Svaki od oblika koji su navedeni, manifestira se putem nekoliko načina počinjenja ili se čak međusobno kombiniraju.

Kada je u pitanju način zloporabe ukradenih ili izgubljenih platnih kartica, u pravilu, kriminalci platnu karticu, do koje dođu počinjenjem kaznenih djela, odmah zloporabljuju, i to najčešće na prodajnim mjestima, tako što ukradenom karticom plaćaju robu sve dok kartica ne bude blokirana od izdavatelja, ili dok transakcija ne bude odbijena zbog nedostatka sredstava na računu. Ako kriminalci i dođu do PIN koda kartice, nju je moguće zloporabiti i na bankomatima. Način i mjera zloporabe kartice ovise i o tome je li u pitanju debitna ili kreditna kartica, Classic ili elektronička, je li s magnetskom trakom ili čipom, je li inozemna ili domaća i tako dalje; kao i o vremenskom roku u kojem će banka biti obaviještena o izgubljenoj/ukradenoj kartici a da bi blokirala njezinu uporabu.

Svi znamo, a posebno kriminalci, da će krađa ili gubitak kartice biti brzo prijavljen banci, pa u cilju «kupovine» vremena u kojem će zloporabiti karticu pribjegavaju prijevarama. S obzirom na to da kriminalci raspolažu podacima o oštećeniku, stupaju s njim u kontakt predstavljajući se kao pošteni pronalazač, dogovaraju mjesto i vrijeme vraćanja kartice koje po potrebi i produljuju. Za to se vrijeme trude maksimalno iskoristiti karticu. Čak i u slučaju kada banka blokira karticu, plativa je u inozemstvu, te je odnose izvan granica i zloporabe u više manjih iznosa do kojih se ne provodi autorizacija plaćanja, ili u slučaju da posjeduju i PIN kod kartice, uzimaju gotov novac s bankomata.

Iskusniji kriminalci ukradenu ili pronevjerenu karticu vraćaju vlasniku, ali prethodno pribave podatke s kartice kopiranjem magnetske trake što se obavlja skimingom, odnosno uporabom uređaja koji se zove skimer.[8] Skimer je malen ali kompleksan uređaj veličine kutije šibica koji optički čita i pohranjuje podatke s magnetskog zapisa.

Kriminalci izrađuju, na osnovi kopiranog magnetskog zapisa, lažnu platnu karticu koju nazivaju «siva», «bijela» ili «zlatna» plastika. Ovakve zloporabe mogu se spriječiti pravovremenim prijavljivanjem nestanka kartice banci, kako bi ona bila blokirana i zadržana u

[8] Eng. *Skimming devices* – posebna je oprema ili uređaj kojim se prepisuje zapis sadržan na magnetskoj pisti platne kartice. Ovakav uređaj – skimer, može biti različitih oblika i dimenzija u zavisnosti od mjesta gdje se postavlja i načina korištenja.

bankomatu, odnosno oduzeta na prodajnome mjestu. Krađa neuručene platne kartice koju banka korisniku dostavlja putem pošte, kao što smo već prije rekli, predstavlja jedan od oblika zloporabe kartica. Iz sigurnosnih razloga PIN za karticu dostavlja se odvojeno od kartice. Zloporaba neuručenih kartica može se spriječiti, a sigurnost dostave povećati obveznim dostavljanjem kartice preporučenom poštom s povratnicom, te se na isti način može dostaviti i PIN kod.

Neovlaštena uporaba tuđe platne kartice najčešće se obavlja posudbom od osoba kojima je tuđa kartica dostupna. Spomenute obavljaju plaćanje ili podižu novac na teret računa vlasnika bez njegova odobrenja ili znanja. Zabilježeni su slučajevi kada članovi uže obitelji neovlašteno uporabljuju tuđu karticu. Na isti je način moguće provesti skiming podataka.

Svaku zloporabu, pa i ovu, treba odmah prijaviti banci kako bi banka blokirala karticu. Prevencija ovakvih zloporaba prije svega jest u čuvanju PIN koda kojeg vlasnik kartice ne bi trebao nikome povjeriti. Prevencija na prodajnim mjestima sastoji se u uspoređivanju potpisa na slipu i kartici; a u slučaju bilo kakve sumnje, ispravno je da trgovac na uvid zatraži osobnu iskaznicu kupca i odbije transakciju, te pritom zadrži karticu i obavijesti policiju.

Kada je u pitanju samo izrada i zloporaba platnih kartica, to se obavlja nakon neovlaštenog pribavljanja podataka prave kartice. Kao što smo već rekli, radi se tehnikom skiminga (krađe; snimanja kartičnih podataka). Podaci se nakon skiminga jednostavno prenose na magnetsku traku lažne kartice. Skiming je prijevara koja podrazumijeva izradu falsifikata kartice na osnovi kopiranja zapisa s magnetske trake.

Nažalost, skiming se može obaviti na apsolutno svim mjestima na kojima se rabe platne kartice i sve češće ga radi skupina zaposlenih u akceptantskoj mreži, s obzirom na to da su skimeri vrlo malih dimenzija i sastoje se od čitača, memorije i napajanja. Konobari, prodavači, taksisti – potencijalni su sudionici u skimingu kartica, naravno, uz određenu proviziju.[9]

Zloporaba platnih kartica predmet je organiziranog kriminala i kao počinitelji javljaju se profesionalci koji u većini slučajeva imaju veće znanje o platnim karticama negoli sami djelatnici u banci; i zbog toga predstavljaju veliku opasnost za same izdavatelje kartica.

Kada je riječ o prevenciji zloporaba lažnih kartica, mora se provoditi u više faza i na više nivoa, kako od strane samog vlasnika kartice tako i od strane prodavača ili davatelja usluge, ali i od strane same banke koja je izdavatelj kartice. U novije vrijeme, u cilju ranog otkrivanja eventualnih zloporaba, rabi se sustav obavještavanja o transakcijama putem SMS poruke koja stigne na mobilni telefon.

Zloporabe i prijevare koje počine akceptanti odnosno trgovci, obavljaju se unaprijed promišljenim korištenjem tuđih ili lažnih platnih kartica i to češće u većim iznosima. Obavljaju se samostalno ili u dogovoru s kriminalcima. U ovom slučaju trgovci prihvaćaju plaćanje ukradenim karticama uz određenu proviziju. Ovdje je motiv čisto koristoljublje jer banka s kojom su sklopili ugovor o prihvaćanju plaćanja karticama, obavit će uplatu na račun trgovca iako je plaćanje obavljeno zloporabom kartice. Veći stupanj ovakve prijevare jest otvaranje lažnog prodajnog mjesta. U tom slučaju lažni trgovac otvara prodajno mjesto samo da bi s bankom sklopio ugovor na osnovi kojeg mu se instalira POS-terminal. Kasnije čini zloporabe uporabom platnih kartica. Preventivne mjere u ovome slučaju trebaju biti usmjerene na provjere trgovca prije postavljanja POS-terminala i na monitoring njegova poslovanja.

[9] Kresoja, M. i Kirkov, Z. (2009), Prevencija pranja novca u bankarskom poslovanju, Zbornik radova, Internacionalna asocijacija kriminalista, Sarajevo, str. 191.

Kada je u pitanju zloporaba koju čine sami korisnici, može se zamijetiti nekoliko pojavnih oblika. Prvi je davanje lažnih podataka prilikom apliciranja za izdavanje platne kartice (u tom se slučaju rabi i lažna dokumentacija); drugi je oblik obavljanje plaćanja karticom ili podizanje novca na bankomatu u većim iznosima a da se lažno prijavi banci da mu je kartica ukradena ili zloporabljena. I na kraju, korisnik može rabiti debitnu platnu karticu za koju ne osigurava pokriće u ugovorenome roku.

Prevencija se sastoji u provjeri podataka o potencijalnom korisniku i monitoringu nad uporabom kartice. Dokaz da je on osobno a ne netko drugi koristio platnu karticu, može biti i snimka s videonadzora bankomata ili mjesta plaćanja.

Navedene oblike zloporabe možemo nazvati i «ručnim radom». Elektroničke zloporabe mnogo su složenije i zahtijevaju viši stupanj znanja iz područja informatike. Na primjer, jedan oblik jest i korištenje softverske aplikacije koja generira moguće brojeve platnih kartica i kao takva obavlja više uzastopnih pokušaja autorizacije na određenim sajtovima.[10]

Drugi oblik je takozvano *pecanje*, odnosno hvatanje brojeva platnih kartica koje se rabe na internetu dok pravi korisnici platnih kartica plaćaju robu ili usluge putem interneta. Postoje lažni sajtovi koji služe samo za to da bi neoprezni korisnici ostavili podatke platne kartice, što predstavlja oblik moguće prijevare ili zloporabe.

Danas, za kupnju bilo čega preko interneta kupcu nije potrebna platna kartica u fizičkom obliku već su dovoljni samo podaci kartice: broj, mjesec i godina isteka i CVV broj. Počinitelji kaznenih djela do ovih podataka o platnim karticama dolaze na nekoliko načina: slanjem *spamova* ili neželjenih poruka, pecanjem (*phishing*), farmingom (*pharming*) i krađom podataka o platnim karticama iz baze podataka elektroničkih trgovina.

*Spamanje* ili slanje neželjenih elektroničkih poruka obavlja se slanjem velikog broja istih elektroničkih poruka na određeni broj primatelja. Ovaj oblik zloporabe ne predstavlja nikakav trošak pri počinjenju kaznenih djela, osim kada je pribavljanje liste primatelja elektroničke pošte u pitanju. Putem ovakvih poruka šire se i maliciozni softveri kao što su kompjuterski virusi. S pomoću metoda socijalnog inženjeringa, primatelja poruke navodi se da unese svoje podatke u polja za unos koja su predviđena ili u samoj poruci ili preko poslanih linkova (poveznica).

Pecanje predstavlja najčešći oblik pribavljanja povjerljivih podataka o platnim karticama u posljednjim godinama. Pecanje podrazumijeva skup aktivnosti kojima neovlaštene osobe korištenjem lažnih elektroničkih poruka preko elektroničke pošte i lažnih internetskih stranica financijskih institucija korisnike interneta navode na otkrivanje povjerljivih podataka kao što su jedinstveni matični broj, korisničko ime, lozinka, PIN broj kartice, broj kreditne kartice i tome slično. Pri pecanju, rabi se kombinacija socijalnog inženjeringa i tehničkih mogućnosti koje pružaju suvremene informacijske tehnologije. Za realizaciju ovakvih napada rabe se elektroničke poruke kao što su:

- lažne poruke administratora u kojima se traže korisnički podaci kao što je lozinka,
- lažna upozorenja banaka ili drugih financijskih organizacija da će doći do gašenja računa klijenta ukoliko on ne unese određene podatke,

[10] Kresoja, M. i Kirkov, Z. (2009), Prevencija pranja novca u bankarskom poslovanju, Internacionalna asocijacija kriminaliteta, Sarajevo, str. 193.

- poruke koje obavještavaju korisnika da je dobio na lutriji zbog čega treba dostaviti određene podatke kako bi mogao podići dobitak,
- poruke koje pozivaju na sigurnost i od korisnika zahtijevaju otkrivanje osobnih podataka ili traže instalaciju nekog programa radi otklanjanja otkrivenog sigurnosnog propusta.[11]

Prijevara koja se naziva *phishing* ili pecanje realizira se na vrlo jednostavan način. Na primjer, na *mail* adresu korisnika pošalje se poruka okvirno ovog sadržaja: «S obzirom na preuređenje baze podataka (ime banke) banke, molimo Vas da se putem linka ulogirate na sajt i popunite tražene podatke.» U slučaju da je primatelj *maila* zaista komitent (nalogodavac) navedene banke, događa se najčešće i da ode na navedeni link. Tada se otvara lažna *web*-stranica banke koja po svim karakteristikama izgleda kao prava. Ponuđene su opcije za unos podataka: ime, prezime, JMBG, adresa, broj telefona, i broj kartice koja se rabi zajedno sa CVV brojem. Nakon unosa podataka, najčešće se dobije poruka «pogrešna vrsta kartice, ponovite unos»; naivni korisnici tada unose podatke svih kartica koje posjeduju. Krađa identiteta može se izvesti i korištenjem pisama koja se šalju korisnicima kartica, međutim, elektronička verzija daleko je jeftiniji način.

S obzirom na to da je korisnička svijest o ovakvim prijevarama na većem nivou, počinitelji kaznenih djela primorani su upotrijebiti neke nove tehnike. Umjesto slanja elektroničkih poruka, danas se rabe virusi tipa *trijan keylogger, mouce loggers* i *screen grabers,* kako bi od žrtava prijevara preuzimali osjetljive podatke.

Farming ili *pharming* vrsta je prijevare koja se realizira preusmjeravanjem protoka podataka s originalnog *web-sajta* na lažnu mrežnu stranicu. Do prijevare s karticama dolazi prilikom konektiranja korisnika na *sajt* financijske institucije ili banke. Prilikom tipkanja adrese *sajta* u određenom dijelu procesuiranja zahtjeva, prije konekcije na željeni sajt dolazi do redirekcije na klonirani *sajt* koji izgleda identično originalnom. Ostali dio unosa podataka sličan je kao i kod «pecanja». Razlika je u tome što je kod pecanja meta napada veliki broj individualnih žrtava koje se napadaju jedna po jedna, dok se u *farmingu* u vrlo kratkom vremenu napada ogroman broj internetskih korisnika.

Ovaj napad razlikuje se od «pecanja» po tome što napadač ne mora navoditi korisnika da pritisne hipervezu u elektroničkoj poruci; čak i ako korisnik točno unese URL adresu u zadano polje internetskog pretraživača, napadač ga i dalje može preusmjeriti na krivotvorenu lokaciju. Iz tog je razloga i uvedeno novo ime (*pharming*) kako bi se napravila razlika između ovih dviju vrsta napada. Farming se obično izvodi tehnikama otimanja DNSa ili takozvanog trovanja DNS keša. Postoje dva tipa farminga. Prvi je način sljedeći: uz pomoć virusa "trojanca" mogu se izmijeniti podaci na udaljenom serveru (poslužitelju). To je *prist* tekstualni fajl koji predstavlja ostatak iz prethodne povijesti interneta, kada je rabljen da bi povezao internetsku adresu s adresom nekog računala. Ova prva tehnika koristi modifikaciju ovog fajla kako bi povezala adrese poznatih banaka i drugih financijskih institucija sa IP adresom *phishing sajta*, tako da, kada korisnik otvori pretraživač i u polje za pretragu utipka naziv svoje banke, umjesto da ode na pravi *sajt*, biva prebačen na lažni.

Drugi tip farminga koristi slabu točku u funkcioniranju, u ovom slučaju DNSa. DNS

[11] Amidžić – Macanović, S. (2012), Zloupotrebe i prevare korištenje platnih kartica, Internacionalna asocijacija kriminalista, Banja Luka, str. 58.

mijenja ulogu lokalnog *fajl hosta* pri spajanju internetske adrese sa IP adresom korisnika. Kada korisnik unese internetsku adresu u polje pretraživača, na DNS serveru traga se za njom i ukoliko pravi server ne prepozna IP adresu, on zahtjev prenosi drugom serveru sve dok se ne pronađu rezultati pretrage. Problem je u tome što ovi protokoli dopuštaju da se pored zadanih kriterija za pretrage, u povratku sa servera dodaju i neke druge informacije, pa tako počinitelji ovih kaznenih djela, kada pošalju lažnu elektroničku poruku koja sadrži *phishing* stranicu, a kada DNS server, nakon što korisnik ode na lažni link, potraži tu stranicu preko interneta, i poveže se na URL prave banke, praktično vraćaju kao dio pretrage lažnu *phishing* stranicu. Svaki put kada korisnik proba obaviti novu pretragu, biva prebačen na lažnu stranicu.

Kada je u pitanju krađa podataka o platnim karticama iz baze podataka elektroničkih trgovina, može se reći da veliki broj baza podataka koje se danas rabe u poslovne svrhe imaju neku formu internetskog *interfejsa* a na taj način dopuštaju internim i/ili vanjskim korisnicima da im lako priđu kroz komercijalne softvere za pretraživanje.

Često se događa da se baze podataka u kojima se nalaze osobni podaci o korisnicima usluga kompromitiraju upravo ovim putem, s obzirom na to da nisu dovoljno zaštićene.[12]

Većina internetskih stranica elektroničkih trgovina napravljena je na PHP ili My SQL baziranim softverima. Glavni cilj ovih internetskih stranica jest osiguranje proizvoda i usluga klijentima. Ovakvi *sajtovi* uglavnom su interaktivni i zasnovani su na principu poštovanja želja korisnika i odgovora na njihove upite. Najčešći od načina preuzimanja kontrole nad internetskom stranicom napadi su SQL injekcijama i *ceoss-site scripting*. SQL injekcijama u sustav baze podataka ubacuje se mali dio podataka ili programski kod koji istražuje slabosti u zaštiti same baze podataka, da bi se kasnije nesmetano zloporabile radi kompromitiranja i krađe podataka s platnih kartica.

*Cross-site scripting* predstavlja tip slabosti kompjutorskog sustava vezanog uz internetske aplikacije koje dopuštaju da počinitelji kaznenih djela ubace kod u internetsku stranicu koju posjećuju drugi korisnici. Otkrivene slabosti u skriptama internetskih stranica mogu biti iskorištene od napadača koji na taj način zaobilazi kontrolu pristupa internetskoj stranici.

Elektroničke trgovine preko svojih internetskih stranica na našem području za naručivanje robe uglavnom traže osnovne podatke kao što su broj telefona, ime, prezime i adresa osoba gdje će se preuzeti roba...; također, traži se broj platne kartice i CVV2 broj kao i osobni podaci vlasnika. Počinitelji kaznenih djela najčešće naručuju skupocjenu robu koju nakon počinjenja kaznenog djela mogu lako i brzo preprodati.

Kako bi ostali anonimni, počinitelji kaznenih djela ostavljaju lažne podatke na *sajtu*, kao kontakt elektroničke adrese ostavljaju adrese otvorene na internetskim servisima koji omogućavaju *web*-baziranu poštu, gdje je teško dobiti podatke o vlasnicima jer se serveri nalaze u inozemstvu.

Na našim prostorima, za skrivanje identiteta počinitelja na internetu, rabe se pristupi na javnim mjestima, kao na primjer u *cyber* cafeima, knjižnicama, fakultetima i slično, s obzirom na to da se posjetitelji ovih servisa vrlo često identificiraju jedinstvenom oznakom koja predstavlja samo generalni identifikator određenog računala ili mjesta konekcije. Ovakvi servisi često se ne mogu povezati s identitetom osoba koje su ih koristile, ako mjesto nije

[12] Kresoja, M. i Kirkov, Z. (2009), Prevencija pranja novca u bankarskom poslovanju, Internacionalna asocijacija kriminaliteta, Sarajevo, str. 195.

snimano, ako nema svjedoka i slično; a osobe koje ih koriste imaju potpuni pristup internetu i to gotovo uvijek bez ikakvih ograničenja. Također, korištenje bežičnih tehnologija za pristup internetu dovelo je do ekspanzije ovakvih zloporaba.[13]

U daljem tekstu bit će predočen kraći osvrt na kazneno djelo falsificiranja i zloporabe platnih kartica u zakonodavstvima država Zapadnog Balkana. U Srbiji na platnim karticama postoji četvoroznamenkasti PIN kod, koji je uvijek nužan da bi se rabio bankomat, ali prilikom *online* kupnje on je nepotreban. Zakoni na osnovi kojih se regulira poslovanje upotrebom platnih kartica u Srbiji jesu:

- Krivični zakonik Republike Srbije
- Zakon o platnom prometu
- Zakon o bankama i drugim financijskim organizacijama.

Na osnovi Krivičnog zakonika Republike Srbije reguliraju se sva kaznena djela koja se odnose na falsificiranje i zloporabu platnih kartica, članak 225. ovog Zakona; kao i bilo koja uporaba platnih kartica bez pokrića, članak 228. stavak 1. ovoga Zakona. Na osnovi spomenutoga Zakona predviđene su odgovarajuće kazne za počinitelje kaznenih djela.

U Krivičnom zakoniku Republike Crne Gore kazneno djelo falsificiranja i zloporabe platnih kartica nalazi se u skupini kaznenih djela protiv platnog prometa i gospodarskog poslovanja. Spomenuto kazneno djelo propisano je u članku 260. U tome smislu, članak 260. stavak 1. propisuje da "*ko napravi lažnu platnu karticu ili ko preinači pravu platnu karticu u namjeri da je upotrijebi kao pravu, ili ko takvu lažnu platnu karticu ili tuđu pravu platnu karticu koja je neovlašćeno pribavljena nabavi, drži ili prenese radi upotrebe ili takvu karticu upotrebi, kazniće se zatvorom do tri godine*". Dakle, možemo zaključiti da je u prvom stavku ujedinjeno i kazneno djelo falsificiranja i kazneno djelo zloporabe, u odnosu na KZ Republike Srbije, gdje je u posebnom stavku regulirana zloporaba platne kartice (članak 225. stavak 4. KZ-a RS).

Kada je riječ o falsificiranja platnih kartica u Kaznenom zakonu Republike Hrvatske, ono je regulirano kaznenim djelom falsificiranje isprave u članku 278. Dakle, kod ovih kaznenih djela objekt zaštite jest vjerodostojnost isprave. Stavak 1. propisuje da će se osoba koja napravi lažnu ispravu, preinači ispravu, upotrijebi lažnu ispravu kao pravu i nabavi lažnu ispravu radi upotrebe, kazniti zatvorom do tri godine. Stavak 2. propisuje da će se osobe koje obmane drugog o sadržaju kakve isprave i potpisivanju takve isprave, držeći da potpisuje drugu ispravu, kazniti zatvorom do tri godine. Stavak 3. propisuje posebnu zaštitu javne isprave, mjenice, čeka, platne kartice, javne ili službene knjige; te osobe koje počine radnju iz prvog i drugog stavka – bit će kažnjene kaznom zatvora od šest mjeseci do pet godina.

U Krivičnom zakonu Bosne i Hercegovine u članku 257. inkriminirano je kazneno djelo falsificiranja kreditnih i ostalih kartica bezgotovinskog plaćanja. Spomenuto kazneno djelo nalazi se u grupi kaznenih djela protiv gospodarstva, poslovanja i sigurnosti platnog prometa. Naime, u stavku 1. opisan je osnovni oblik. Pa tako, tko s ciljem, da je upotrijebi kao pravu, izradi lažnu kreditnu karticu ili drugu karticu bezgotovinskog plaćanja, ili tko preinači takvu pravu karticu, ili tko takvu lažnu platnu karticu upotrijebi kao pravu, kaznit će se kaznom zatvora do tri godine. Stavak 2. propisuje kvalificirani oblik u slučaju da je radnjom iz stavka

[13] Amidžić – Macanović, S. (2012), Zloupotrebe i prevare korištenjem platnih kartica, Internacionalna asocijacija kriminalista, Banja Luka, str. 69.

1. pribavljena imovinska korist i navodi da će se počinitelj kazniti kaznom zatvora do pet godina. Stavak 3. propisuje također kvalificirani oblik u slučaju da je pribavljena imovinska korist koja prelazi vrijednost od deset tisuća konvertibilnih maraka. U tom slučaju, počinitelj će se kazniti kaznom zatvora od jedne do osam godina. Stavak 4. propisuje najteži oblik kaznenog djela falsificiranja kreditnih i ostalih kartica bezgotovinskog plaćanja i to u situaciji kada je pribavljena imovinska korist koja prelazi pedeset tisuća konvertibilnih maraka. Propisana kazna za ovaj oblik jest zatvor u trajanju od dvije godine do deset godina. Stavak 5. propisuje da će se lažne kreditne kartice i kartice za bezgotovinsko plaćanje oduzeti.

Prijevare i krivotvorenje bezgotovinskih sredstava plaćanja ozbiljna su prijetnja sigurnosti EU-u jer su veliki izvor prihoda organiziranog kriminala i njima se omogućuju druge kriminalne aktivnosti poput terorizma, krijumčarenja droga i krijumčarenja ljudi. Europol navodi da nezakonitim tržištem za plaćanje karticama u EU-u dominiraju dobro strukturirane skupine organiziranog kriminala koje djeluju na globalnoj razini, koje godišnje ilegalno zarade najmanje 1,44 milijarda eura (razina kartičnih prijevara koje procjenjuje Europska središnja banka). Taj se iznos može povećavati, uglavnom zbog sve veće digitalizacije gospodarstva i stvaranja novih instrumenata platnog prometa s pomoću tehnoloških inovacija. Osim toga, bezgotovinska plaćanja bitna su za internetske transakcije, a njihova je sigurnost ključna za uspostavu jedinstvenog digitalnog tržišta. S druge pak strane, prijevare u području bezgotovinskog plaćanja uzrokuju velike izravne gospodarske gubitke (na primjer, zračni prijevoznici godišnje gube otprilike 1 milijardu USD na svjetskoj razini zbog kartičnih prijevara) i smanjuju povjerenje potrošača, što može dovesti do smanjene gospodarske aktivnosti i ograničenog sudjelovanja na jedinstvenom digitalnom tržištu. Zašto Komisija predlaže novu Direktivu o prijevarama u području bezgotovinskog plaćanja? Tehnološki razvoj, primjerice sve veća upotreba mobilnog plaćanja ili virtualnih valuta, doveli su do značajnih promjena u području bezgotovinskog plaćanja i povećanja internetskih prijevara. Kako bi se osigurao učinkoviti kazneni progon počinitelja kaznenih djela s pomoću novih instrumenata, EU-ov okvir kaznenog prava mora se ažurirati kako bi se osiguralo usklađivanje razine kazni. Naime, budući da se prijevare u području bezgotovinskog plaćanja često događaju na internetu, tradicionalni pojam teritorijalnosti doveden je u pitanje jer se sustavi za informacije mogu upotrebljavati i kontrolirati na daljinu s bilo kojeg mjesta. Stoga bi trebalo uvesti nadležnost za počinjena kaznena djela bez obzira na državljanstvo počinitelja i njegovu fizičku prisutnost, ali uzimajući u obzir štetu koju je prouzročilo kazneno djelo počinjeno na državnom području države članice. Iako se postojećom okvirnom odlukom o borbi protiv prijevare i krivotvorenja bezgotovinskih sredstava plaćanja pridonijelo stvaranju zajedničkog okvira EU-a o kaznenom pravu, trenutačna razina usklađenosti nije dovoljna da bi se na odgovarajući način poduprle prekogranične istrage i kazneni progoni.

## 3. ZAKLJUČAK

Na samome kraju ovoga rada, može se zaključiti da je ljudsko društvo krajem prošlog i početkom ovoga stoljeća doživjelo najbrže promjene u svojoj povijesti. U spomenutome razdobolju promijenjen je način funkcioniranja mnogih djelatnosti, nastupile su promjene u strukturi rada, na tržištu itd. Navedene promjene stvorile su društvo koje je bazirano na, između ostalog, znanosti, znanju, informacijama, inovacijama, informacijskoj tehnologiji i tome slično. Također, ove tehnologije omogućavaju brži protok roba i usluga. Ekspanzija

tehnologije dovela je do promjena u području platnog prometa, do promjena načina plaćanja i izmjene strukture sredstava plaćanja u kojoj je sve manji udio gotovog novca i klasičnih sredstava bezgotovinskog plaćanja. Međutim, pojavom prvih platnih kartica počele su i prve zloporabe sredstava plaćanja.

Zloporaba platnih kartica predmet je organiziranog kriminala i kao počinitelji javljaju se profesionalci koji u većini slučajeva imaju veće znanje o platnim karticama nego sami djelatnici u banci, te zbog toga predstavljaju veliku opasnost za same izdavatelje kartica.

Suzbijanje ovih pojava činjenja kaznenih djela zloporaba i prijevara na štetu banke i korisnika ove vrste bankarskih usluga, moguće je uz primjenu suvremenih kriminalističkih metoda i sredstava. Nizom preventivnih mjera može se utjecati na smanjenje kriminala.

## LITERATURA

1. Amidžić – Macanović, S. (2012). Zloupotrebe i prijevare korištenjem platnih kartica, Internacionalna asocijacija kriminalista, Banja Luka.
2. Aglietta, M., Orlean, A. (2002). Novac – između sile i povjerenja, Mate d.o.o. i Zagrebačka škola ekonomije i menadžmenta, Zagreb.
3. Božina, L. (2003). Novčana ekonomija – novac i bankarstvo, Fakultet ekonomije i turizma "dr. Mijo Mirković" Pula, Pula.
4. Božina, L. (2008). Novac i bankarstvo, Fakultet ekonomije i turizma "dr. Mijo Mirković" Pula, Pula.
5. Božina, L. (2008). Monetarna teorija i politika, Fakultet ekonomije i turizma "dr. Mijo Mirković" Pula, Pula.
6. Đokić, Z. (2008). Falsifikovanje i zloupotrebe platnih kartica, zbornik radova, Internacionalna asocijacija kriminalista, Brčko.
7. Krapac, D. (2010). Kazneno procesno pravo. Prva knjiga: Institucije. IV. Izdanje. Zagreb: Narodne novine.
8. Kresoja, M. i Kirkov, Z. (2009). Prevencija pranja novca u bankarskom poslovanju, Internacionalna asocijacija kriminala, Sarajevo.
9. Klačmer Čalopa, M., Cingula, M. (2009). Financijske institucije i tržišta kapitala, TIVA FOI, Varaždin.
10. Horjan, A. M. (2003). Kreditne kartice i njihova zloporaba. Policija i sigurnost, 12(1-3), 75.-82.
11. Pavišić, B., Modly, D., Veić, P. (2006). Kriminalistika 1. Zagreb: Golden marketing.
12. Pena, U. i Pantić, S. (2019). Falsifikovanje i zloupotreba platnih kartica, Zavod za udžbenike i nastavna sredstva, Istočno Novo Sarajevo.
13. Perić, V. (1987). Oblici operativne djelatnosti službe javne sigurnosti. Zagreb: RSUP.
14. Popovska Kamnar, N. (2014). Korištenje elektroničkog novca i njegov utjecaj na monetarnu politiku, JCEBI 1(2).
15. Rose, P. S., Hudgins, S. C. (2015). Upravlajnje bankama i financijske usluge, Mate d.o.o., Zagreb.
16. Ružić, D., Biloš, A. i Turkalj, D. (2014). E – marketing, Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet, Osijek.

17. Sabol, Ž. (2003). Identitet rukopisa – sudska grafologija. Zagreb: Hrvatska: Lexsis.
18. Singer, M. (1996). Kriminologija. Zagreb: Nakladni zavod Globus.
19. Vasković, V. (2007). Sustavi plaćanja u elektronskom poslovanju, Fakultet organizacionih nauka, Beograd.
20. Zečević, M. (2009). Bankarstvo, Evropski Univerzitet Beograd, Beograd.
21. Zelenika, R. (1998). Metodologija i tehnologija izrade znanstvenog i stručnog rada. Rijeka: Tipograf d.d.

Summary

**Damir Bilić**

**Misuse of payment cards**

Crime in the area of misuse and forgery of payment cards is of recent date, and it can be announced that everything is represented. Like cash, payment cards can be the subject of criminal theft, fraud or other criminal offences against property (aggravated theft, robbery, robbery, theft and the like). The global spread of payment cards, the ease of use and the easy accessibility of modern technologies, make these cards extremely attractive to criminals or organised crime groups.

**Keywords:** payment cards, ATM, theft, skimming, fishing, electronic banking, electronic or digital money.