Revija za kriminalistiko in kriminologijo / Ljubljana 63 / 2012 / 2, s. 123-135

Zlorabe plačilnih kartic - pogledi izdajateljev kartic

Igor Lamberger[*], Bojan Dobovšek[**], Boštjan Slak[***]

Članek predstavlja nekatera najsplošnejša znamenja, lastnosti in predpostavke, ki spremljajo zlorabe plačilnih kartic (npr. organizirani kriminal, ključne pomanjkljivosti pri varnosti kartic, uspešnost standardov pri zagotavljanju varnosti itd.), ter želi empirično preveriti, ali te lastnosti držijo v očeh zaposlenih, ki se ukvarjajo z izdajanjem plačilnih kartic in imajo najboljši vpogled v problem. Prvi del zajema klasičen pregled literature, drugi del pa statistično obdelane podatke, ki smo jih pridobili z anketo med zaposlenimi na področju izdaje plačilnih kartic. Pregled literature, izkušnje iz prakse (oboje je botrovalo sestavi anketnega vprašalnika) in empirična overitev so pokazali, da nekatere značilnosti držijo (mednarodni storilci, prenos kriminalitete, magnetni trak kot šibka točka). Pokazalo se je tudi, da vloga represije ni tako občutna, kot bi pričakovali. Zaradi omejenega števila izdajateljev kartic in s tem povezanega manjšega števila oseb, zaposlenih na tem področju, smo bili soočeni z določnimi težavami pri izvajanju bolj specifičnih statističnih analiz, saj se je razmerje med številom anketiranih in številom spremenljivk pokazalo kot precej omejujoče. Za nadaljnje raziskave predlagamo kvalitativno raziskovanje (intervjuje ali analize primerov).

Ključne besede: plačilne kartice, kreditne kartice, zlorabe, zaščita, represija

UDK: 343.37:343.85

1 Uvod – teoretična izhodišča

Plačilne kartice so plačilni instrument, ki za razliko od gotovine predstavlja večjo uporabnost, saj lahko z njim plačujemo izdelke in storitve neodvisno od valute na daljavo (internetno plačevanje) in pri uporabi kreditnih kartic brez trenutno razpoložljivih finančnih sredstev. Prav slednje predstavljajo prve zametke plačilnih kartic in segajo že v leto 1800, ko so trgovci in finančni posredniki dajali izdelke ali proizvode na kredit, toda šele po letu 1900 so se pojavile papirnate kartice, ki so jamčile za kredit in so jih izdajali hoteli, večje trgovine ali drugi ponudniki storitev svojim najpomembnejšim strankam (Woolsey in Gerson, 2009). Čeprav so se primarno uveljavile kreditne kartice oziroma kartice z odloženim plačilom, so se s časom pojavile še druge vrste plačilnih kartic; tako še danes delimo plačilne kartice na debetne kartice (ang. debit cards), kreditne kartice (ang. credit cards), kartice z odloženim plačilom, razvijajo pa se kartice s prednaloženo vrednostjo (Predplacnik.si, 2011).

Brezgotovinsko plačevanje, ki ga omogočajo plačilne kartice, se je v sodobnem plačilnem prometu tako zelo razvilo, da ponekod že presega gotovinsko plačevanje. Sodobne plačilne kartice imenujemo tudi »plastični denar«, saj se pojavljajo v obliki standardiziranih plastičnih kartic, z vtisnjenim (izbočenim) zapisom podatkov, magnetnim (podatkovnim) zapisom in zapisom v elektronskem vezju (t. i. čip).[1] Vsi trije zapisi vsebujejo vse podatke o imetniku kartice, banki izdajateljici in možnosti plačevanja ter dvigovanja gotovine na bančnih avtomatih. Ti referenčni podatki, shranjeni na magnetnem traku in/ali čipu, se primerjajo s podatki v evidenčni centralni bazi pred opravljanjem transakcije.

Tako kot vse ostale plačilne instrumente tudi plačilne kartice že od samega začetka spremljajo zlorabe, prevare, goljufije in podobna dejanja, katerih pravna kvalifikacija je včasih celo zamujala. Dober primer je Slovenija, kjer je ustrezna pravna kvalifikacija zlorab in ponarejanja plačilnih kartic v veljavi šele od 1. 11. 2008, ko je stopil v veljavo KZ-1.

Zlorabe sodobnih plačilnih kartic se lahko zgodijo v katerem koli delu procesa njene uporabe; celo pri izdajanju plačilne kartice, kadar si goljufi pridobijo plačilno kartico z osebnimi podatki tretje osebe. Pri tem gre za t. im. krajo identitete. Oseba, katere identiteta je bila zlorabljena, to ugotovi

[*] Igor Lamberger, doktor ekonomskih znanosti, zaposlen na Generalni policijski upravi v Policijski akademiji kot predavatelj in zunanji sodelavec (višji predavatelj) Fakultete za varnostne vede Univerze v Mariboru; igor.lamberger@policija.si

[**] Bojan Dobovšek, izredni profesor in prodekan na Fakulteti za varnostne vede Univerze v Mariboru; Bojan.Dobovsek@fvv.uni-mb.si

[***] Boštjan Slak, podiplomski študent Fakultete za varnostne vede Univerze v Mariboru.

[1] Vpeljava tehnologije čip je proizvod standarda EMV (Europay, MasterCard, Visa), ki se zavzema za uporabo tehnologije čip + PIN. Možna kombinacija za avtorizacijo je tudi čip + podpis.

šele, ko na njen naslov začnejo prihajati računi za poplačilo dolga (Maniam in Earl, 2006; Rizzardi, 2008). Nadalje so se zlorabe dogajale, ko so kriminalci oropali ali okradli poštne ali kurirske uslužbence, ki so nosili plačilne kartice do njihovih legitimnih lastnikov (Zupančič, 1999). Zato se danes PIN-številka in plačilna kartica pošiljata ločeno, zahteva pa se potrditev (podpis), da je kartico prevzel legitimni imetnik. Ko je kartica že varno v lastnikovih rokah, se možnosti zlorabe še ne zmanjšajo. V grobem lahko razdelimo zlorabe v štiri skupine: (1) zlorabe imetnika, do katerih pride zaradi neustreznega ravnanja imetnika kartic(e); (2) zloraba izgubljene ali ukradene kartice, kar je pogosto posledica nepazljivosti lastnika kartice ali tatvine/ropa/vloma; (3) zlorabe s ponarejenimi karticami, v sodobnem času druga najpogostejša oblika zlorab plačilnih kartic; večjo varnost onemogoča različnost varnostnih in tehnoloških standardov v svetu; (4) zlorabe z ukradeno identiteto, v sodobnem času naraščajoča in ponekod že prevladujoča oblika zlorab plačilnih kartic z vrsto pojavnih oblik.

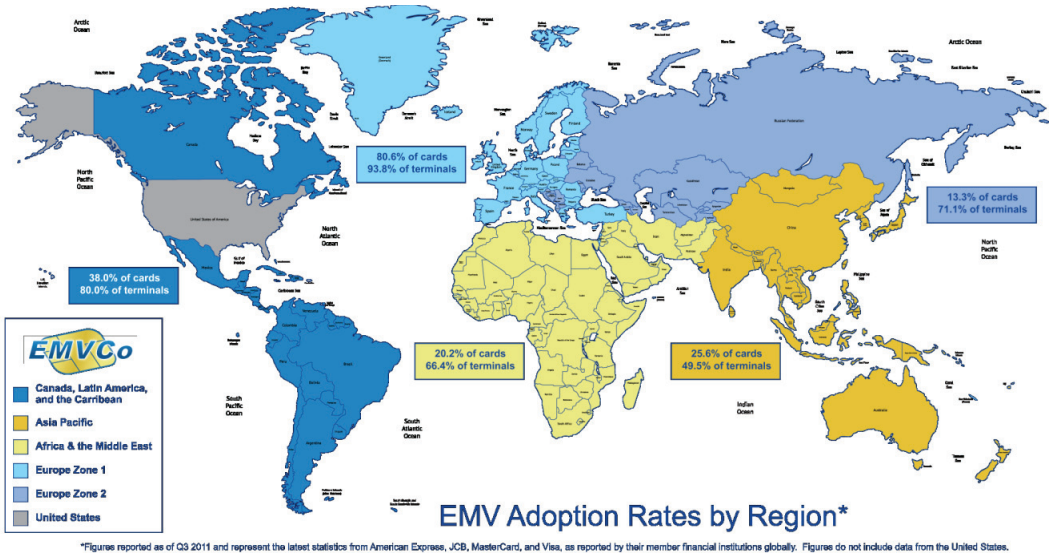
Zlorabe plačilnih kartic že od začetka spremljajo določene preventivne dejavnosti in represivni odzivi, hkrati pa jim pripisujejo tudi določene atribute oziroma določene neempirične in iz prakse (ne)potrjene lastnosti. Na primer, da so zlorabe plačilnih kartic del organizirane kriminalitete, da legitimni lastnik ne more zlorabiti kartice, da je treba ogromno tehničnega znanja za izvedbo zlorabe plačilne kartice, da je tehnična zaščita edina možna zaščita, da je lastnik izključno sam odgovoren za zlorabo ipd. Naloga članka je, da s pomočjo pregleda literature predstavi te domneve in jih z empirično raziskavo potrdi ali ovrže.

1.1 Preprečevanje zlorab plačilnih kartic

Ukrepi za zaščito plačilnih kartic se prekrivajo z varnostnimi ukrepi izdajateljev plačilnih kartic, katerih želja je, da bi uspešno kombinirali učinkovitost kartice (hitrost uporabe, zanesljivost) z njeno varnostjo. Primarna metoda shranjevanja podatkov na plačilnih karticah je bila metoda embosiranja - vtisnjeni, izbočeni podatki, ki so nosili najosnovnejše informacije o plačniku (ime in priimek, datum veljavnosti kartice in številka računa). S ponarejanjem teh podatkov (izdelava identičnih kartic) je storilec lahko na preprost način nakupoval večinoma dražje, luksuzno blago (Lamberger, 2011). Kasneje so karticam zaradi informatizacije poslovanja dodali magnetni trak, na katerem so prav tako shranjeni vsi ključni podatki. Te je mogoče precej lahko prebrati, kopirati in tako tudi zlorabiti. Varnost magnetnega traku se ni z leti nič izboljšala, v zadnjem času pa ga je nadomestila čip tehnologija shranjevanja podatkov, ki je izredno varen način uporabe plačilnih kartic in uspešno zmanjšuje število zlorab (Prabowo, 2011). Po drugi strani pa magnetni trak, ki je še vedno v rabi, predstavlja ključno šibko točko kartic (Berghel, 2007; Lamberger, 2009), saj se zaradi globalno še ne vpeljane tehnologije po standardu EMV na karticah ohranja (Wiese in Omlin, 2009), kar lahko primerjamo s situacijo, ko imamo »najboljša protivlomna vrata, a pustimo okno odprto«.[2] Stanje vpeljave čip tehnologije je razvidno iz spodnje slike (Slika 1). Podatki za ZDA na sliki niso vidni, saj se, kot navaja King (King, 2012), čip tehnologija v tej državi le počasi vpeljuje. EMV-kartice so bile izdane v nekakšnih pilotnih programih, namenjene pa so predvsem tistim, ki veliko potujejo v tujino. Če upoštevamo dejstvi, da imajo prebivalci ZDA po najmanj dve plačilni kartici in da jih večina ne potuje na tuje, gre za majhen del zajetih oseb.

Zaradi uvedbe čip tehnologije se je poleg spremembe modusa operandi zgodilo tudi, da se storilci sedaj zatekajo k drugačnim oblikam zlorab plačilnih kartic, kjer predvsem izkoriščajo kibernetski prostor. Gre za t. i. »card-not-present schemes« (Wiese in Omlin, 2009; Prabowo, 2011; King, 2012). Zaradi zagotavljanja višje stopnje varnosti kartic lahko predvidevamo (prve analize v tujini to tudi kažejo), da se bo še povečalo število tistih zlorab, za izpeljavo katerih ni potrebna dejanska posest kartice in PIN-številke (Wiese in Omlin, 2009; Prabowo, 2011). Včasih je dovolj, da si storilci pridobijo le številke s plačilne ali kreditne kartice, ki jih potem navedejo pri internetnem ali ponekod zelo priljubljenem telefonskem nakupovanju (Ghosh in Reily, 1994; Aleskerov, Fieisleben in Rao, 1997; Berghel, 2007;Wiese in Omlin, 2009; Sullivan, 2010; Montague, 2011). Podatke za tovrstne zlorabe storilci pridobijo s tatvino osebnih predmetov (torbic, denarnic) ali z neustrezno uničenih ali shranjenih odrezkov poročil, bančnih izpiskov ipd., ki jih pridobijo tudi z brskanjem po smeteh (Albrecht, Albrecht, in Tzafrir, 2011); lahko pa podatke pridobijo z računalniškim vdorom v sistem, kjer so ti podatki shranjeni (Maniam in Earl, 2006; Sullivan, 2010; Montague, 2011; Albrecht, Albrecht, in Tzafrir, 2011), npr. z vdorom v sistem trgovske/gostinske verige (Liebowitz, 2011)

[2] "Skimming", (nedovoljeno kopiranje podatkov s kartice za zlorabo) je do sedaj skoraj vedno potekal s kopiranjem podatkov v magnetnem zapisu. Od uvedbe čipa je takšno kopiranje oteženo (nismo zaznali primera, ko bi storilci kopirali podatke s čipa) in storilci so spremenili svoj modus operandi, tako da namesto da skopirane podatke uporabijo v državi, kjer je kartica bila kopirana, te podatke pošljejo sostorilcem v države, kjer čip tehnologija še ni vpeljana (EUROPOL: Major international network of payment card fraudsters dismantled, 2011). Čeprav je skoraj v vseh državah EU že vpeljana čip tehnologija, je klasičen skimming v letu 2009 na področju EU povzročil za več kot 350 milijonov evrov škode (EURPOLReview: General report on EURPOL Activities za 2009). Storilci v večini primerov namestijo naprave za kopiranje na bančne avtomate ali pa imajo notranjo pomoč v restavracijah in trgovinah, kjer uslužbenci poleg na POS-terminalih »povlečejo« kartico tudi čez "skimming" napravo. Zaradi svetovnega tehnološkega napredka je sedaj mogoče naprave za kopiranje namestiti na POS-terminal, ne da bi se uslužbenci tega zavedali (Sullivan, 2010).



Slika 1: Stanje vpeljanega EMV-standarda (vir: EMV Adoption rates 2011, 2011)

ali v podatkovni sistem podjetij, ki poslujejo s plačilnimi karticami (Dnevnik: Anonimni naj bi ukradli več kot milijon dolarjev in jih dali v humanitarne namene, 2011).[3] Lažne strani bank in spletnih trgovin zavedejo kupce, ki vnesejo podatke svojih kartic v spletne obrazce in tako omogočajo zlorabe.[4] Nekateri avtorji štejejo to obliko za največjo nevarnost kartičnih zlorab (Prabowo, 2011). To potrjuje tudi analiza škode, saj so v zadnjih nekaj letih takšne prevare prevladovale oziroma povzročile največ škode v Veliki Britaniji (Fraud The Facts 2011, 2011), Franciji (Annual Report of The Observatory For Payment Card Security, 2010), Avstraliji (Payments fraud in Australia, 2011) in Kanadi (Credit Card Fraud Statistics, 2010). Škoda, povzročena s tovrstnimi zlorabami, pa se je zmanjšala v Veliki Britaniji (Fraud The Facts 2011, 2011), zlasti zaradi različnih programskih rešitev in t. i. »3D Secure«, dodatnega gesla, ki se uporablja pri spletnem nakupovanju (Financial Fraud Action UK, 2012). Nekatere druge države pa izdajatelji kartic šele spodbujajo k uvajanju »3D Secure« gesel. Sekundarno je pomemben celovit informacijski sistem izdajateljev kartic in upravljavcev informacijskih sistemov, ki učinkovito deluje v realnem času.

Vsi pomembnejši izdajatelji plačilnih kartic naj bi uporabljali t. i. »neural technology«, ki zazna spremembe v vzorcu uporabe kartice (Aleskerov, Fieisleben in Rao, 1997; Wiese in Omlin, 2009).

Pri vzpostavitvi sistema, ki v takšni ali drugačni meri obravnava plačilne kartice, se srečamo z vrsto standardov. Najpoglavitnejši je t. i. PCI-standard. V bistvu je PCI-standard proizvod zaveze petih največjih izdajateljev plačilnih kartic (VISA, MasterCard, American Express, Discover Financial Services in JCB International) za varnejše in sistematizirano poslovanje pri uporabi plačilnih kartic. Gre za zbirko obveznih priporočil, ki so jih dolžni uveljaviti vsi, ki želijo uporabljati kartične storitve. Priporočila zajemajo obvezna navodila pravnim osebam (trgovcem in podobnim ponudnikom storitev), izdajateljem kartic in drugim za ustrezno izdelavo informacijskega sistema, vodenja sistema in varnostnih politik za zaščito podatkov in informacij, ki se nanašajo na plačilne kartice (pci-standard.com, 2012; PCI Security Standards Council, 2012). Čeprav gre za zbirko dobrih in učinkovitih standardov, se trend zlorab plačilnih kartic ni občutno umiril, čeprav zametki PCI-standarda segajo že v leto 2006. Študija, ki jo je naredilo podjetje Imperva, sicer kaže, da standard prinaša večjo varnost, toda določena podjetja bolj verjamejo, da je včasih varnost posledica

[3] Največja podjetja že dolgo namenjajo pozornost varovanju svoje lastnine in varovanje največkrat zaupajo privatnim varnostnim podjetjem. Več pozornosti se v zadnjem času namenja varovanju informacijskega sistema podjetja, pri čemer to nalogo opravlja določen sektor v podjetju. Lahko bi rekli, da gre za pod-obliko zasebnega varovanja in sicer za obliko privatnega »in-house« varnostnega servisa, katerega naloga je zagotavljanje varnosti lastnemu podjetju (Sotlar, 2009).

[4] Po svetu se pojavlja vrsta zlorab (phising, spoofing, ipd.), katerih podroben opis pa ni namen tega članka. Bernik in Meško (2011) ugotavljata, da javnost, kot najbolj nevarne grožnje na spletu prepoznava tiste, o katerih mediji najpogosteje poročajo, ki pa niso nujen odsev realnosti. Povrhu vsega tovrstno poročanje le redko ozavešča o načinu varne rabe spleta.

več dejavnikov in ne samo prilagojenosti standarda (PCI DSS Trends 2010: QSA Insights Report, 2010; PCI DSS Compliance Trends Study, 2011, 2011). Tako mnenje je lahko posledica problemov, ki spremljajo vpeljavo PCI-standarda. Na primer dejstva, da podjetjem določa, kako zelo intenzivno se morajo podrediti standardu na podlagi števila letnih kartičnih transakcij (več transakcij – več zahtev morajo izpolnjevati) (Mann, 2011), do tega, da je za trgovce drag (Segal, Ngugi in Mana, 2011). Zato se opredelijo za manjše trgovce in tako zmanjšajo število zahtev. Gre lahko tu za vprašanje poštenosti? Saj ni vse, kar je dovoljeno, tudi pošteno, ob čimer se zdi, da nasploh v današnjem kapitalističnem času tovrstne »prebrisanosti« ne prinašajo ne družbene manjvrednosti, še redkeje pa pravne sankcije (Tičar, Bohinc, in Nahtigal, 2010). Stroški vpeljave standarda so resnično lahko zelo visoki, so pa podjetja potem zavarovana in jih, če so vpeljali PCI-standarde, manj ali sploh ne kaznujejo ob vdoru (Vellayan, 2011). Kompleksnost, ki ga standard zahteva, je tako obsežna, da so celo najboljši informacijski sistemi v skladu s standardom zgolj 30–40 % (Mann, 2011). Problem je tudi dejstvo, da je bil PCI-standard grajen za tehnologijo magnetnega zapisa in se enkripcija podatkov zahteva le za tisti njihov del, ki se prenaša prek javne mreže (Segal, Ngugi in Mana, 2011). Treba je upoštevati pametno terminološko ločevanje institucije Verizon glede PCI-standarda; ta razločuje med *skladnostjo* s standardom in *potrjevanjem* standarda: »Skladnost je stalen proces doseganja regulativnega standarda, medtem ko je potrjevanje občasen dogodek, ki poskuša meriti in opisati stopnjo upoštevanja standarda (2011 Data Breach Investigations Report, 2011, s: 62). Gre torej za sicer teoretično dober standard pri tistih, ki morajo izpolnjevati več zahtev,[5] včasih pa je bolj izgovor za prelaganje odgovornosti kot sredstvo za dejansko preprečevanje zlorab.

Ključno je tudi sodelovanje in preventivno delovanje tistih, ki jim je storitev namenjena, to je trgovcev in ostalih ponudnikov storitev. Ti ne delujejo preventivno, saj vedno bolj opuščajo preverjanje istovetnosti lastnika kartice (Downing Jr.in Geller, 2009) z npr. preverjanjem podpisa, čeprav ta metoda še vedno precej dobro deluje (Matyáš, Krhovják, Kumpost in Cvrcek, 2008).

[5] Segal, Ngugi in Mana (2011) navajajo, da je v skupini podjetij, ki se morajo najmanj podrediti standardu, okoli 6 milijonov podjetij, ki izvedejo zgolj samoevalvacijo skladnosti s standardom. Medtem pa je na spletu možno najti tudi nekaj primerov vdorov v sisteme, ki so dosegali PCI-standard, npr. Heartland Payment Systems (Heartland data breach proves PCI compliance is not enough, 2009). Verisonova študija vdorov navaja, da je 11 % podjetij, zajetih v študijo, doživelo vdor v sistem, skladen s PCI-standadom (2011 Data Breach Investigations Report, 2011). Dvomi v učinkovitost so torej več kot upravičeni, saj se je treba zavedati preprostega dejstva, da so novi standardi zgolj reaktiven odgovor na določeno obliko vdora ali zlorabe.

1.2 Represija in zlorabe plačilnih kartic[6]

Ob odpovedi zaščitnih mehanizmov se vključijo represivne institucije s svojimi aktivnostmi. Vloga represivnih organov je v večini primerov nedvoumna, neproblematična, a hkrati tudi raznolika. Primarna naloga je preprečiti nadaljevanje zlorabe, poiskati storilca, ga ustrezno kaznovati in vsaj deloma povrniti škodo oškodovancu.[7] Država oz. oblast skuša vplivati na kriminaliteto tudi z represijo. Eden izmed dejavnikov zmanjšanja kriminalitete je strogo, hitro in zanesljivo delovanje vseh institucij formalnega družbenega nadzorstva. Problem je v tem, da ima generalna zaščita, torej kazenske sankcije, kot opozorilo vsem potencialnim storilcem kaznivih dejanj le minimalen, če ne zgolj »mitični« učinek (Pečar, 2002).

Atributi, ki spremljajo represivne ukrepe pri zlorabah plačilnih kartic, so po eni strani v določeni meri odvisni od podtipa zlorabe, po drugi pa predstavljajo nekakšen vsesplošni pogled na zlorabe. Pri pregonu kaznivih dejanj zlorab plačilnih kartic se tako srečamo z vrsto problemov, saj imajo tovrstna kazniva dejanja značilnosti gospodarske (kjer je preiskovanje oteženo zaradi kompleksnosti, prikritosti in nevidnosti) (Gradišar in Lamberger, 2010) in organizirane kriminalitete (transnacionalno delovanje)[8] (Zupančič, 1999). Tako kot za ostala kazniva

[6] Nadgradnja članka Gradišar, M., in Lamberger, I. (2010). Vpliv represivnih dejavnikov na zlorabe kreditnih in plačilnih kartic v Sloveniji. Revija za kriminalistiko in kriminologijo 61(1).

[7] V Sloveniji v skladu z Zakonom o plačilnih storitvah in sistemih (ZPlaSS) (členi 116 do 120) uporabnik nosi škodo do 150 evrov, ostalo pa ponudnik plačilnih storitev, razen kadar uporabnik naklepno ali iz hude malomarnosti ni izpolnil razumnih ukrepov za varovanje svojih plačilni instrumentov.

[8] Vrsto značilnosti je moč najti v definiciji organizirane kriminalitete, ki jo navajajo Meško, Dobovšek in Kešetović, kjer tako organizacijo sestavljajo posamezniki, ki delujejo skupaj, da bi ustvarili dobiček z nelegalnimi dejavnostmi. Značilnosti so opazne tudi v zvezi s prevzetim pojmom »organizirana kriminaliteta«. Slovenija ga je prevzela od Europola, ki pravi, da lahko govorimo o organizirani kriminaliteti, ko so izpolnjeni štirje obvezni kriteriji (1. združba vsaj treh ljudi, 2. deluje v daljšem časovnem obdobju, 3. cilj je premoženjska korist (dobiček) ali družbena moč, 4. izvrševanje težjih kaznivih dejanj (uradno pregonljivih kaznivih dejanj) in dva od sedmih neobveznih kriterijev (1. uporaba nasilja in /ali korupcije, 2. delovanje na mednarodni ravni, 3. vpletenost v pranje denarja, 4. uporaba notranjih pravil ravnanja, 5. točno določena delitev vlog in nalog za člane, 6. uporaba podjetniškega načina delovanja, 7. vplivanje na medije, gospodarstvo, državno upravo, politiko) (Načrt ukrepov kriminalistične policije za omejevanje organizirane kriminalitete za obdobje od 2005 do 2007). Značilnosti organizirane in transnacionalne kriminalitete potrjujejo tudi analiza primerov ter Eurpolova poročila, kjer je pogosto omenjena mreža storilcev s transnacionalnim delovanjem (EUROPOL Review: General report on EURPOL Activities za 2009; EUROPOL: Major international network of payment card fraudsters dismantled, 2011).

dejanja s področja gospodarske kriminalitete je tudi za zlorabe kreditnih in plačilnih kartic značilno, da so kazenski postopki v primeru prijetja in sankcioniranja storilcev sorazmerno dolgi, grozi zastaranje kazenskega pregona storilca zaradi preteka časa in da je relativno malo storilcev s tega področja kriminalitete pravnomočno obsojenih. Pravnomočno zaključenim obsodilnim sodbam morajo slediti tudi odvzemi protipravno pridobljenih finančnih koristi, saj ta ukrep pomeni, da se kriminal ne izplača, ker odkrit in obsojen storilec od storitve kaznivega dejanja nima koristi (Lamberger, 2009).

Še večja je kompleksnost zlorab plačilnih kartic v primerih, ko zlorabo povzroči (legitimni) imetnik kartice. V pogodbi se ob prejetju kartice zapišejo pogoji in pravila poslovanja ter določen znesek limita. Prav v povezavi z limitom se zgodi največ zlorab imetnikov kartic. Ti namreč včasih zavestno ali nezavedno zahajajo v negativno stanje in tako kljub doseženemu limitu še naprej dvigujejo gotovino ter plačujejo blago ali storitve. Z uvedbo elektronskih POS-terminalov je to sicer težje (a ob določenih pogojih še vedno možno), pogosto pa uporabljajo več kartic in tako zaidejo v dolgove, ki jih niso zmožni poravnati. In čeprav včasih resnično nimajo nobenega namena poravnati dolgov, povzročenih z uporabo kartice, je lahko tovrstno stanje tudi posledica šibke finančne samokontrole in potrošniške miselnosti (Ghosh in Reily, 1994). V Sloveniji to sicer ni tako pogost pojav, problem pa je v ZDA, kjer se s problemom (pre)zadolženosti, ki je rezultat neustrezne rabe kreditnih kartic, ukvarja celo predsednik (Fightmaster, 2009). Zaznati je mogoče povečano število reformnih politik, ki bi ustrezneje in bolje uredile področje kreditiranja (in s tem tudi izdajanja kreditnih kartic) v ZDA (Stadler, 2012). Podobne probleme imajo še v Veliki Britaniji (Richards, Palmer, in Bogdanova, 2008), na Novi Zelandiji in drugje (Maniam in Earl, 2006). Veliki dolgovi so lahko tudi posledica nepričakovanih dogodkov. Gre torej za širša družbena vprašanja, kjer je vloga represivnih organov vprašljiva, saj tehnično gledano ni motiva in naklepa, ki sta vsaj v Sloveniji nujen element pri pravni kvalifikaciji.

2 Metoda

Da bi preverili mnenje oseb, ki se dnevno ukvarjajo z izdajanjem kartic, o trenutnih zaščitnih in represivnih metodah, smo konec maja 2008 opravili raziskavo. Vanjo smo vključili osebe, zaposlene na področju varnosti elektronskega bančništva ali pa tiste, ki se izobražujejo in usposabljajo ter dnevno ukvarjajo z zahtevami na tem področju, izvajajo dejavnosti za zmanjšanje zlorab - strokovnjake torej, ki največ vedo o preprečevanju zlorab in zagotavljanju varnosti na tem področju.[9]

Uporabili smo anketni vprašalnik, ki smo ga v elektronski obliki (kot MS Officov Wordov dokument) poslali osebi za stike na Združenju bank Slovenije. Ta ga je posredovala zaposlenim v institucijah, ki se ukvarjajo z elektronskim bančništvom. Ti so izpolnjene vprašalnike poslali nazaj osebi za stike, ki jih je posredovala izvajalcu ankete; identiteta anketirancev, ki bi se videla iz pošiljateljevega elektronskega naslova, je tako ostala skrita. Anonimnosti in dostopnosti zaposlenih se drugače ni dalo zagotoviti, saj prihajajo iz vsaj dvajsetih bank oz. institucij, ki se ukvarjajo s področjem plačilnega prometa. Dostop do bančnikov je neposredno prek banke skoraj nemogoč. Vse osebe, ki jim je bil poslan vprašalnik, so ga vrnile izpolnjenega.

Anketni vprašalnik je bil sestavljen iz treh vsebinskih sklopov. Prvi je splošen oz. posnetek stanja na tem področju (obseg elektronskega plačevanja, pojavnost zlorab ipd.), drugi je s področja preventivnih (varnostni mehanizmi na karticah, ključne slabosti, tehnološke rešitve ipd.), tretji pa represivnih dejavnikov (vloga in uspešnost represivnih organov pri pregonu, vloga sankcioniranja ipd.). Gre za trditve, ki smo jih oblikovali glede na izkušnje, prakso in na podlagi ugotovitev literature. Anketirance smo spraševali, kako se strinjajo s postavljenimi trditvami. Strinjanje so ocenjevali s petstopenjsko Likertovo lestvico z odgovori: (1) sploh se ne strinjam, (2) se ne strinjam, (3) se strinjam, (4) se večinoma strinjam, (5) se popolnoma strinjam. Odgovori anektiranih so bili obdelani s statističnim programom SPSS 12.0.

3 Rezultati

Pridobili smo mnenje 43 zaposlenih pri izdajateljih in procesorjih, ki se ukvarjajo s področjem plačilnih kartic (v nadaljevanju: zaposleni). Tako je bilo zajetih približno 80 % vseh zaposlenih v bankah in drugih podjetjih (npr. Diners), ki se dnevno ukvarjajo z izdajanjem plačilnih kartic. Število vseh zaposlenih na tem področju je okoli 53. Podatek je iz Združenja bank Slovenije, katerega članice so skoraj vse poslovne banke v Sloveniji. Tabela 1 predstavlja podrobnejše značilnosti vzorca.

[9] Izjavo lahko podkrepimo z dejstvom, da obstaja vrsta konferenc in mednarodnih srečanj, kjer so poglavitne teme zlorabe plačilnih kartic. Številne banke imajo neke vrste analitikov, ki pozorno spremljajo in analizirajo vse v povezavi s prevarami in banko/podjetjem (Whitmore, 2010; ATM Security 2012, 2012).

Tabela 1: Karakteristike vzorca

Karakteristike vzorca (n=43)		Frekvenca	Odstotek [%]
Spol	Ženski	14	32,6
	Moški	22	51,2
	Ni odgovora	7	15,3
Starost	20–29	1	2,3
	30–39	16	37,2
	40–49	14	32,6
	50–59	11	25,6
	Nad 60	1	2,3
Izobrazba	Srednja	13	30,2
	Višja	5	11,6
	Visoka	9	20,9
	Univerzitetna	14	32,6
	Magisterij in več	2	4,7
Skupna delovna doba [leta]	0–10	4	9,3
	11–19	15	34,9
	20–29	12	27,9
	30–39	12	27,9
Delovna doba na področju kartičnega prometa [leta]	0–10	19	44,2
	11–19	17	39,5
	20–29	5	11,6
	30–39	2	4,7

Prvi sklop vprašalnika je anketirane spraševal o trenutnem stanju obravnavne tematike.

Tabela 2: Pregled stanja na področju brezgotovinskega plačevanja

Trditev		Ocena strinjanja s trditvijo					Skupaj	M[10]	SD[11]
		(1)	(2)	(3)	(4)	(5)			
s1: Brezgotovinski plačilni promet se bo v prihodnje povečal.	n			3	3	37	43	4,79	0,56
	%			7,0	7,0	86,0	100		
s2: Zlorabe na tem področju se z večanjem obsega poslovanja povečujejo.	n		4	6	16	17	43	4,07	0,96
	%		9,3	14,0	37,2	39,0	100		
s3: Ponarejanje kartic je lažje kot ponarejanje denarja.	n		9	12	12	10	43	3,53	1,08
	%		20,9	27,9	27,9	23,3	100		
s4: Plačilne kartice morajo biti zavarovane z varnostnimi elementi.	n				3	40	43	4,93	0,26
	%				7,0	93,0	100		
s5: Največjo nevarnost za ponarejanje predstavlja magnetni zapis na kartici.	n		2	10	10	21	43	4,16	0,95
	%		4,7	23,3	23,3	48,8	100		
s6: Pravila poslovanja uporabnikov s karticami morajo biti jasno določena.	n				5	38	43	4,88	0,32
	%				11,6	88,4	100		
s7: Zlorabe s karticami se dogajajo povsod po svetu.	n		2		7	34	43	4,70	0,71
	%		4,7		16,3	79,1	100		
s8: Pravila poslovanja s karticami morajo biti mednarodno primerljiva.	n				11	30	41	4,73	0,45
	%				26,8	73,2	100		
s9: Pogodba med izdajateljem kartic in prodajnim mestom z vidika preprečevanja zlorab je preohlapna.	n	1	1	20	14	7	43	3,58	0,88
	%	2,3	2,3	46,5	32,6	16,3	100		
s10: Vloga prodajnih mest pri preprečevanju zlorab je pomembna.	n			2	15	26	43	4,56	0,59
	%			4,7	34,9	60,5	100		
s11: Za zmanjšanje zlorab je potrebno usposabljanje zaposlenih na tem področju.	n			3	11	29	43	4,60	0,62
	%			7,0	25,6	67,4	100		
s12: Tehnično-tehnološke rešitve lahko omejijo izvajanje zlorab.	n			2	16	25	43	4,53	0,59
	%			4,7	37,2	58,1	100		
s13: Varnost poslovanja je odvisna tudi od organizacijskih rešitev.	n		1	4	17	20	42	4,33	0,75
	%		2,4	9,5	40,5	47,6	100		
s14: Represivni ukrepi (zagrožene kazni) so pomembni za obnašanje storilcev zlorab.	n	4	7	14	7	11	43	3,33	1,29
	%	9,3	16,3	32,6	16,3	25,6	100		

[10] M = Povprečna vrednost.

[11] SD = Standardni odklon.

Zaposleni, ki imajo najboljši pregled stanja, precej soglasno domnevajo, da bo negotovinski plačilni promet narastel. Pozdravljajo jasnost in določnost pravil poslovanja, predvsem pa menijo, da morajo biti kartice zavarovane z varnostnimi mehanizmi. Pri tem so še kar enotnega mnenja glede magnetnega traku kot šibke točke plačilne kartice. Najmanj je bila potrjena trditev, da kazni vplivajo na vedenje storilcev. Da pomembnejšo vlogo pripisujejo zaščiti kot represiji, je razvidno tudi iz Tabela 3.

Tabela 3: Ocenjevanje trditev glede preventive in zlorabe plačilnih kartic

Trditev		Ocena strinjanja s trditvijo (1)	(2)	(3)	(4)	(5)	Skupaj	M	SD
p1: Učinkovit informacijski sistem, ki dela v realnem času, zmanjša možnost zlorab.	n	/	/	/	13	30	43	4,70	0,465
	%	/	/	/	30,2	69,8	100		
p2: Informacijski sistem mora imeti jasno določene odzive v primerih zlorab.	n	/	/	/	4	39	43	4,91	0,294
	%	/	/	/	9,3	90,7	100		
p3: Dodatna gesla in certifikati povečujejo varnost poslovanja.	n	/	/	2	16	25	43	4,53	0,592
	%	/	/	4,7	37,2	58,1	100		
p4: Vdori v informacijske sisteme povečujejo možnost zlorab.	n	/	/	1	11	30	42	4,69	0,517
	%	/	/	2,4	26,2	71,4	100		
p5: Največjo nevarnost predstavljajo uporabnikovi operacijski sistemi in slaba zaščita pred virusi.	n	/	7	12	16	8	43	3,58	0,982
	%	/	16,3	27,9	37,2	18,6	100		
p6: Pošiljanje podatkov uporabnikov preko e-pošte lahko poveča možnost zlorab (fishing).	n	/	/	4	19	20	43	4,37	0,655
	%	/	/	9,3	44,2	46,5	100		
p7: Nakup prek manj poznanih spletnih strani povečuje možnost zlorab.	n	2	2	9	12	18	43	3,98	1,123
	%	4,7	4,7	20,9	27,9	41,9	100		
p8: Zlorabe podatkov prek lažnih spletnih strani je mogoče zmanjšati z uvedbo varovalnih mehanizmov.	n	/	1	3	18	21	43	4,37	0,725
	%	/	2,3	7	41,9	48,8	100		
p9: Informacijski sistemi, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe.	n	/	/	2	14	26	42	4,57	0,59
	%	/	/	4,8	33,3	61,9	100		
p10: Varnostni elementi na kartici omogočajo uspešno zaščito pred ponarejanjem kartic.	n	1	1	5	27	9	43	3,98	0,801
	%	2,3	2,3	11,6	62,8	20,9	100		
p11: Kartice z vgrajenim čipom bodo zmanjšale možnost za zlorabe.	n	2	/	3	18	20	43	4,26	0,954
	%	4,7	/	7	41,9	46,5	100		
p12: Magnetni zapis tudi po uvedbi čipa pomeni nevarnost za potencialne zlorabe.	n	/	3	6	13	21	43	4,21	0,94
	%	/	7	14	30,2	48,8	100		
p13: PIN-koda pomeni večjo zaščito poslovanja pred zlorabami.	n	/	1	1	17	24	43	4,49	0,668
	%	/	2,3	2,3	39,5	55,8	100		
p14: Uporabnike je treba obveščati o možnostih in nevarnostih zlorab.	n	/	/	2	11	30	43	4,65	0,573
	%	/	/	4,7	25,5	69,8	100		
p15: Dobro obveščen uporabnik skrbneje ravna s kartico.	n	/	1	5	17	20	43	4,30	0,773
	%	/	2,3	11,6	39,5	46,5	100		
p16: Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.	n	/	/	4	6	33	43	4,67	0,644
	%	/	/	9,3	14	76,7	100		
p17: Obnašanje uporabnika ima vpliv na možnost zlorab.	n	/	/	10	13	18	41	4,20	0,813
	%	/	/	24,4	31,7	43,9	100		
p18: Uporabniki morajo sami nadzirati porabo svoje kartice in tako sami odkrivati zlorabe.	n	1	3	23	12	4	43	3,35	0,842
	%	2,3	7	53,5	27,9	9,3	100		
p19: Imetnik kartice ne sme biti oškodovan z zlorabo, za katero sam ni odgovoren.	n	/	/	/	15	28	43	4,65	0,482
	%	/	/	/	34,9	65,1	100		
p20: Dodatne tehnične rešitve na bančnih avtomatih lahko zmanjšajo možnosti zlorab.	n	/	/	2	25	16	43	4,33	0,566
	%	/	/	4,7	58,1	37,2	100		
p21: Tehnična in tehnološka zaščita mora slediti razvoju.	n	/	/	/	1	42	43	4,98	0,152
	%	/	/	/	2,3	97,7	100		
p22: Čip kartice ne bodo v celoti onemogočile možnosti zlorab.	n	/	/	4	19	20	43	4,37	0,655
	%	/	/	9,3	44,2	46,5	100		
p23: Storilci se prilagodijo zaščitnim mehanizmom in najdejo nove načine za izvajanje zlorab.	n	/	/	4	15	24	43	4,47	0,667
	%	/	/	9,3	34,9	55,8	100		
p24: Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	n	/	/	/	12	31	43	4,72	0,454
	%	/	/	/	27,9	72,1	100		
p25: Storilci ne poznajo meja in zato je treba sodelovati s tujimi finančnimi institucijami.	n	/	/	/	10	33	43	4,77	0,427
	%	/	/	/	23,3	76,7	100		
p26: Vloga oskrbnikov bančnih avtomatov in policije je pomembna za odkrivanje storilcev zlorab.	n	/	/	2	11	29	42	4,64	0,577
	%	/	/	4,8	26,2	69	100		
p27: Za uspešno ukrepanje in izsledite storilca je potrebna hitra odzivnost.	n	/	/	1	6	36	43	4,81	0,45
	%	/	/	2,3	14	83,7	100		

p28: Kakovosten pretok informacij o zlorabah povečuje možnost odkritja storilca.	n	/	/	/	9	34	43	4,79	0,412
	%	/	/	/	20,9	79,1	100		
p29: Popolne varnosti poslovanja ni mogoče doseči.	n	/	/	3	12	28	43	4,58	0,626
	%	/	/	7	27,9	65,1	100		

Iz Tabele 3 je razvidno mnenje zaposlenih, da je potreben dobro zasnovan informacijski sistem, ki deluje v realnem času in ima jasno določene odzive ob zlorabah. Pomembna je hitra odzivnost, medinstitucionalno in mednarodno sodelovanje. Varnostni mehanizmi kartic so pomembni, a v celoti gledano, anketirani nimajo vedno največjega zaupanja vanje. Zanimivi sta predvsem dve stvari: prva je ta, da zaposleni nimajo niti uporabnika za najbolj odgovornega za zlorabe niti uporabnikovega operacijskega sistema za ključno šibko točko; druga pa je zavedanje oziroma dejstvo, da nimajo utopičnih pričakovanj glede uspešnosti zaščitnih metod (stoodstotne zaščite in varnosti ni).

3.1 Preverjanje hipotez

S statistično analizo želimo preveriti, ali določene domneve, ki se pogosto nanašajo na zlorabe plačilnih kartic, dejansko tudi statistično držijo. Zastavili smo si vrsto hipotez in jih preverili s t-testom[12] za vsako spremenljivko, zajeto v preveritev hipoteze. Zastavljene hipoteze so:

H[1]: Celovit varnostni model mora upoštevati mednarodno dimenzijo.

Tabela 4: Represivne karakteristike in zlorabe plačilnih kartic

Trditev		Ocena strinjanja s trditvijo					Skupaj	M	SD
		(1)	(2)	(3)	(4)	(5)			
c1: Dobra zakonodaja, ki sankcionira zlorabe, je pomembna za preprečevanje zlorab.	n	/	3	9	14	17	43	4,05	0,95
	%	/	7,0	20,9	32,6	39,5	100		
c2: Storilce zlorab je treba sankcionirati.	n	/	/	/	6	37	43	4,86	0,351
	%	/	/	/	14,0	86,0	100		
c3: Višja zagrožena kazen vodi k zmanjšanju zlorab.	n	2	3	20	13	5	43	3,37	0,952
	%	4,7	7,0	46,5	30,2	11,6	100		
c4: Natančno izvajanje zakonodaje vpliva na bodoče storilce.	n	1	1	10	15	16	43	4,02	0,963
	%	2,3	2,3	23,3	34,9	37,2	100		
c5: Povečanje števila odkritih storilcev vpliva na zmanjševanje izvrševanja zlorab.	n	/	2	15	14	12	43	3,84	0,898
	%	/	4,7	34,9	32,6	27,9	100		
c6: Število obsojenih storilcev vpliva na zmanjšanje števila tistih, ki se odločajo za zlorabe.	n	1	2	14	15	11	43	3,77	0,972
	%	2,3	4,7	32,6	34,9	25,6	100		
c7: Postopek sankcioniranja storilca mora potekati in se zaključiti čim prej po dejanju.	n	/	/	1	10	32	43	4,72	0,504
	%	/	/	2,3	23,3	74,4	100		
c8: Storilci na tem področju so zelo dobro organizirani.	n	/	/	2	15	25	42	4,55	0,593
	%	/	/	4,8	35,7	59,5	100		
c9: Tovrstna kriminaliteta ima elemente organizirane kriminalitete.	n	/	/	/	14	28	42	4,67	0,477
	%	/	/	/	33,3	66,7	100		
c10: Storilci ne smejo obdržati premoženjske koristi, ki so si jo z zlorabo pridobili.	n	/	/	/	2	41	43	4,95	0,213
	%	/	/	/	4,7	95,3	100		
c11: Večina storilcev prihaja k nam iz drugih držav.	n	1		8	17	16	42	4,12	0,889
	%	2,4		19	40,5	38,1	100		

Pregled rezultatov glede represije (Tabela 4) pokaže, da anketirani sicer menijo, da obstaja povezava med represivnimi dejavniki in zlorabami ter da represija vpliva na storilce. Vpliv represivnih dejavnikov pa ni tako velik, kot bi bilo pričakovati. Menijo, da je treba vedenje storilcev sankcionirati, vendar so bolj kot višina zagrožene kazni in število odkritih dejanj pomembni dobra zakonodaja ter natančno, hitro vodenje in končanje postopkov, še posebej odvzem protipravne premoženjske koristi, ki so si jo storilci pridobili z zlorabami. Ugotovitev po pregledu literature je, da storilci prihajajo iz drugih držav, zato imajo tudi zlorabe plačilnih kartic značaj (mednarodnega) organiziranega kriminala.

Zlorabe na področju elektronskega bančništva imajo pogosto značilnosti mednarodnega kriminala, saj storilci največkrat prihajajo iz drugih držav. Zato je potrebno povezovanje izdajateljev kartic (bank) in vseh institucij, ki preiskujejo

[12] $t = \frac{\bar{X} - 3}{s}\sqrt{n}\, t = \frac{\bar{X} - 3}{s}\sqrt{n}$. Pri preverjanjih vseh hipotez bomo ničelno hipotezo zavrnili, če bo vrednost statistike testa hipoteze padla pod kritično vrednost standardizirane normalne slučajne spremenljivke (pri $\alpha = 0,05$).

ter preprečujejo zlorabe.[13] Hipotezo smo preverili na podlagi treh spremenljivk, in sicer:

– Večina storilcev prihaja k nam iz drugih držav.
– Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.
– Storilci ne poznajo meja in zato je treba sodelovati s tujimi finančnimi institucijami.

H_0 in H_1 se torej vežeta na vse tri trditve in velja:

H_0: $\mu \geq 3{,}5$ $\mu \geq 3{,}5$
H_1: $\mu < 3{,}5$ $\mu < 3{,}5$

V Tabeli 5 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja in t-vrednosti za posamezno spremenljivko (N = 42).

Tabela 5: Izvedba T-testa za H[1]

		SD	95 % interval zaupanja		t
			Spodnja meja	Zgornja meja	
Večina storilcev prihaja k nam iz drugih držav.	4,12	0,889	3,84	4,4	4,513
Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	4,71	0,457	4,57	4,86	17,641
Storilci ne poznajo meja in zato je treba sodelovati s tujimi finančnimi institucijami.	4,79	0,415	4,66	4,92	19,443

Iz Tabele 5 lahko ugotovimo, da pri nobeni spremenljivki ne pade vrednost t pod kritično vrednost, zato hipoteze ne zavrnemo.

H [2]: Na uresničevanje modela celovite varnosti vpliva nekaj ključnih dejavnikov, ki zagotavljajo uspešno in učinkovito preprečevanje zlorab.

Kot smo ugotovili v modelu celovite varnosti, obstajajo trije ključni dejavniki, ki najbolj vplivajo na varnost poslovanja in učinkovitost preprečevanja zlorab. To so: izdajatelji kartic, uporabniki, preventivno-kurativni ukrepi in novi načini tehnično-tehnološke zaščite elektronskih sistemov. Hipotezo smo preverili na podlagi naslednjih spremenljivk:

Izdajatelji kartic

– Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.

Uporabniki

– Uporabnike je treba obveščati o možnostih in nevarnostih zlorab.
– Dobro obveščen uporabnik skrbneje ravna s kartico.
– Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.
– Obnašanje uporabnika vpliva na možnost zlorabe kartice.

Preventivno-kurativni ukrepi

– Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.
– Storilce zlorab je treba sankcionirati.

Tehnično-tehnološke zaščite

– Dodatne tehnične rešitve na bančnih avtomatih lahko zmanjšajo možnosti zlorab.
– Tehnična in tehnološka zaščita morata slediti razvoju.

H_0 in H_1 se torej vežeta na vse trditve in velja:

H_0: $\mu \geq 3{,}5$ $\mu \geq 3{,}5$
H_1: $\mu < 3{,}5$ $\mu < 3{,}5$

V Tabeli 6 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja ter t-vrednosti za posamezno spremenljivko (N = 42).

[13] Banke so tako povezane in sodelujejo z domačimi bankami prek Združenja bank Slovenije in mednarodno s tujimi bankami ter lastniki licenc tujih kartic. Policija prek Europola in Interpola sodeluje z drugimi policijami, saj brez mednarodnega sodelovanja in upoštevanja mednarodne dimenzije ni mogoče omejevati, še manj pa preiskovati zlorab na tem področju.

Tabela 6: Izvedba T-testa za H [2]

			95 % interval zaupanja		
		SD	Spodnja meja	Zgornja meja	t
Za preprečevanje in odkrivanje zlorab je potrebno sodelovanje med izdajatelji kartic.	4,73	0,449	4,59	4,87	17,641
Uporabnike je treba obveščati o možnostih in nevarnostih zlorab.	4,66	0,575	4,48	4,84	13,185
Dobro obveščen uporabnik skrbneje ravna s kartico.	4,29	0,782	4,05	4,54	6,81
Tudi uporabniki storitev morajo skrbeti za varnost poslovanja.	4,68	0,65	4,48	4,89	11,95
Obnašanje uporabnika ima vpliv na možnost zlorabe kartice.	4,2	0,813	3,94	4,45	5,475
Dobra zakonodaja, ki sankcionira in opredeljuje zlorabe, je pomembna za preprečevanje zlorab.	4,05	0,947	3,75	4,35	3,772
Storilce zlorab je treba sankcionirati.	4,85	0,358	4,74	4,97	25,445
Dodatne tehnične rešitve na bančnih avtomatih lahko zmanjšajo možnosti zlorab.	4,33	0,566	4,15	4,5	9,569
Tehnična in tehnološka zaščita morata slediti razvoju.	4,98	0,152	4,93	5,02	63,5

Iz Tabele 6 lahko ugotovimo, da pri vseh spremenljivkah vrednost t ne pade pod kritično vrednost, zato hipoteze ne zavrnemo.

H [3]: Sprememba tehnologije zaščite posameznih delov sistemov in celote se mora prilagajati ter nadgrajevati z razvojem tehnično-tehnoloških novosti na področju zaščit sistemov.

Zaradi potrebne in zahtevane večje varnosti pri opravljanju plačilnega prometa ter pri prenosu finančnih transakcij po informacijskih sistemih je zahtevana visoka stopnja varnosti sistemov in naprav, ki omogočajo opravljanje transakcij (bančni avtomati, POS- terminali, plačilne kartice…). Hipotezo smo preverili na podlagi naslednjih spremenljivk:

– dodatna gesla in certifikati povečujejo varnost poslovanja;
– zlorabe podatkov prek lažnih spletnih strani je mogoče zmanjšati z uvedbo varovalnih mehanizmov;
– informacijski sistemi, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe;
– varnostni elementi na kartici omogočajo uspešno zaščito pred ponarejanjem kartice;
– kartice z vgrajenim čipom bodo zmanjšale možnosti za zlorabe;

H_0 in H_1 se torej vežeta na vseh pet spremenljivk in velja:

$H_0: \mu \geq 3,5 \ \mu \geq 3,5$
$H_1: \mu < 3,5 \ \mu < 3,5$

V Tabeli 7 so prikazane povprečne vrednosti, standardni odkloni, 95 % intervali zaupanja in t-vrednosti za posamezno spremenljivko (N = 42).

Tabela 7: Izvedba T-testa za H [3]

			95 % interval zaupanja		
		SD	Spodnja meja	Zgornja meja	**t**
Dodatna gesla in certifikati povečujejo varnost poslovanja.	4,55	0,593	4,36	4,61	11,472
Zlorabe podatkov prek lažnih spletnih strani je mogoče zmanjšati z uvedbo varovalnih mehanizmov.	4,36	0,727	4,13	4,58	7,893
Informacijski sistemi, ki zaznavajo neobičajno uporabo kartice, pomagajo odkrivati zlorabe.	4,57	0,59	4,39	4,76	11,763
Varnostni elementi na kartici omogočajo uspešno zaščito pred ponarejanjem kartice.	4,02	0,749	3,79	4,26	3,901
Kartice z vgrajenim čipom bodo zmanjšale možnosti za zlorabe.	4,29	0,944	3,99	4,58	5,198

Iz Tabele 7 lahko ugotovimo, da pri vseh spremenljivkah vrednost t ne pade pod kritično vrednost, zato hipoteze ne zavrnemo.

4 Razprava

Ključna sinteza ugotovitev pregleda literature in empirične raziskave kaže na omejeno moč represivnih dejavnikov, ki prinašajo zgolj reaktiven učinek. Ta je seveda nujen in potreben, a vloga represivnih ukrepov za generalno zaščito je skoraj zanemarljiva. Skladna s Pečarjevo (Pečar, 2002) trditvijo o omejenem vplivu zagroženih kazni so tudi mnenja tistih, ki delujejo na področju izdajanja kartic (glede neučinkovitosti zagroženih kazni). Vendar pa menijo, da bi bila generalna zaščita bolj preventivno učinkovita, če bi bile preiskave hitrejše, če bi bil delež pravnomočnih obsodilnih sodnih epilogov večji in če bi sodbi sledil odvzem nezakonito pridobljenega premoženja. Vsi ti zaželeni ukrepi se kažejo skoraj kot utopična ideja, saj je kljub uspehom še vrsta ovir: kompleksnost preiskav, kibernetski prostor, dolgotrajni sodni postopki. Ne samo, da je vedno več zlorab plačilnih kartic na spletu, tradicionalne zlorabe kartic imajo tudi mednarodne značilnosti. To se je pokazalo pri pregledu literature, v praksi in tudi v okviru naše raziskave. Kombinacija teh dejavnikov ima po vsej verjetnosti neki vzajemni učinek. Mednarodni storilci štejejo zlorabe plačilnih kartic za dejanje z majhnim tveganjem in velikim dobičkom. Gre torej za odličen primer kriminološke teorije o dobičku in tveganju kot vzroku za nastanek kriminalitete. Praksa nakazuje, da storilci ob pridobitvi podatkov plačilnih kartic ali finančnih sredstev te nemudoma posredujejo prek spleta ali drugih komunikacijskih sredstev v druge države in se tako znebijo obremenjujočih dokazov ob prijetju. Storilčev status tujca prav tako otežuje preiskavo nacionalnih preiskovalcev.

Kje so torej rešitve? Poleg poudarjenega mednarodnega in medinstitucionalnega sodelovanja, ki je pravzaprav edina uspešna metoda pregona, je odgovor v samozaščitnem delovanju uporabnikov storitev elektronskega bančništva. To pa seveda ni tako lahko. Povprečen uporabnik spleta in plačilnih kartic se velikokrat sploh ne zaveda nevarnosti. Izdajatelji kartic ga verjetno tudi ne bodo izobrazili, saj bi se lahko iz strahu pred viktimizacijo odločil, da ne bo uporabljal storitev, ki jih elektronsko bančništvo omogoča. Pri strokovnjakih, ki imajo bogato znanje s področja informatike, kriminalistike, ekonomije, pa se kot Ahilova peta kaže prav osredotočenost na posamezno področje. Informacijski strokovnjaki, ki se preveč osredotočajo na tehnološke vidike zlorab, se ne posvetijo analizam dejanskih primerov, zato so njihove razvojne ideje že na začetku necelovite. Ekonomisti imajo premalo tehničnega, pravnega in kriminalističnega znanja. Kot evidenten odgovor se tako še naprej kaže medinstitucionalno delovanje. Uspeh izobraževanja uporabnikov se bo verjetno pokazal šele čez desetletje, saj trenutno tisti, ki bodo najbolj vešči tehnologije, šele vstopajo ali deloma že zapuščajo šolske klopi. Za začasno občutno zmanjšanje klasičnih zlorab plačilnih kartic bo dovolj globalno vpeljan EMV-standard, dokler storilci ne najdejo poti za zlorabo podatkov, shranjenih v čipu. Za trenutno naraščajoče zlorabe, kjer ni potrebna dejanska posest kartice (torej t. i. CNP-zlorabe), pa rešitve še ni. Različni spletni protokoli in standardi, ki so reaktiven proizvod iznajdljivosti storilcev, bodo škodo uspešno zmanjševali za določen čas, dokler storilci ne bodo našli odgovora tudi nanje.

Raziskovanje zlorab plačilnih kartic bi tako še naprej moralo biti v interesu strokovne in akademske javnosti in v

čim bolj povezanem sodelovanju med njima. Oblika kvantitativnega raziskovanja se je pokazala kot omejujoča, zato predlagamo kvalitativno raziskovanje, več črpanja spoznanj iz praktičnih in raziskanih primerov, z dodatkom kriminoloških in viktimoloških spoznanj, saj ti dve vedi sledita razvoju tehnologije in kibernetski prostor prepoznavata kot določeno polje nevarnosti in tveganj. Predvsem pa sta zanimivi za raziskovalce. Gre za dela, katerih spoznanja bi bilo smiselno povezati z zlorabami plačilnih kartic.

Kako črna prihodnost nas čaka na tem področju, je očitno odvisno od izdajateljev kartic, ki pogosto zaradi stroškov razvoja ustreznih preventivnih metod teh ne spodbujajo ali uvajajo. Dejstvo je, da se provizija in stroški obdelave transakcije obračunajo, pa če je transakcija legitimna ali ne.

Literatura

1. *2011 Data Breach Investigations Report.* (2011). Prevzeto 10. februarja 2012 iz VERIS: http://www.verizonbusiness.com/Products/security/risk/
2. Albrecht, C., Albrecht, C., in Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. *Journal of Financial Crime,* 18(4), 405–414.
3. Aleskerov, E., Fieisleben, B., in Rao, B. (1997). CARDWATCH: A Neural Network Based Database Mining Systern for Credit Card Fraud Detection. *Proceedings of the IEEEIAFE 1997 Computational Intelligence for Financial Engineering* (str. 220–226).
4. *Annual Report of The Observatory For Payment Card Security.* (2010). Prevzeto 10. februarja 2012 iz http://www.banque-france.fr/observatoire/telechar/gb/2010/rapport-annuel-OSCP-2010-gb.pdf
5. *ATM Security 2012.* (2012). Prevzeto 10. februarja 2012 iz RBR: http://www.rbrlondon.com/events/security/view?searchterm=fraud
6. Berghel, H. (2007). Credit Card Forensics: Decoding the magnetic attraction of criminals to swiping. *Digital Village*, 50(12), 11–14.
7. Bernik, I., in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, 62(3), 242-252.
8. *Credit Card Fraud Statistics.* (2010). Prevzeto 20. februarja 2012 iz CBA: http://www.cba.ca/contents/files/statistics/stat_creditcard-fraud_en.pdf
9. *Dnevnik: Anonimni naj bi ukradli več kot milijon dolarjev in jih dali v humanitarne namene*. (2011). Prevzeto 28. januarja 2012 iz Dnevnik: http://www.dnevnik.si/novice/svet/1042497964
10. Downing Jr, C. O., in Geller, E. (2009). Behavior Analysts Address Credit-Card Fraud. *Behavior Analysis Digest International*, 21(4), 13–14. *EMV Adotion rates 2011*. (2011). Prevzeto 3. februarja 2012 iz EMVCo: http://www.emvco.com/images/EMVCo_WorldMap.png
11. *EUROPOL Review: General report on EURPOL Activities za 2009*. (2011). Prevzeto 28. decembra 2011 iz https://www.europol.europa.eu/sites/default/files/publications/europolreview2009.pdf
12. *EUROPOL: Major international network of payment card fraudsters dismantled*. (2011). Prevzeto 28. decembra 2011 iz https://www.europol.europa.eu/content/press/major-international-network-payment- card-fraudsters-dismantled-1001.
13. Fightmaster, M. (2009). *President Obama to meet with credit card execs*. Prevzeto 3. marca 2011 iz DailyFinance.com: http://www.dailyfinance.com/story/president-obama-to-meet-with-credit-card-execs/1525783/
14. *Financial Fraud Action UK.* (2012). Prevzeto 10. februarja 2012 iz http://www.financialfraudaction.org.uk/
15. *Fraud The Facts 2011.* (2011). Prevzeto 10. februarja 2012 iz Financial Fraud Action UK: http://www.financialfraudaction.org.uk/download.asp?file=2696
16. Ghosh, S., in Reily, D. L. (1994). *Credit Card Fraud Detection with a Neural-Network. System Sciences, 1994. Vol.III: Information Systems: Decision Support and Knowledge-Based Systems, Proceedings of the Twenty-Seventh Hawaii International Conference,*. Hawaii International Conference (str. 621–630). Wailea, HI, USA.
17. Gradišar, M., in Lamberger, I. (2010). Vpliv represivnih dejavnikov na zlorabe kreditnih in plačilnih kartic v Sloveniji. *Revija za kriminalistiko in kriminologijo,* 61(1), 28–36.
18. *Heartland data breach proves PCI compliance is not enough.* (2009). Prevzeto 10. februarja 2012 iz ComputerWeekly.com: http://www.computerweekly.com/news/2240088114/Heartland-data-breach-proves-PCI-compliance-is-not-enough
19. King, D. (2012). *Chip-and-PIN: Success and Challenges in Reducing Fraud.* Prevzeto 3. februarja 2012 iz Retail Payments Risk Forum: http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf
20. Lamberger, I. (2009). Vpliv represivnih organov in generalne prevencije na področju zlorab kreditnih in plačilnih kartic, v: *Zbornik povzetkov, 10. slovenski dnevi varstvoslovja*, Fakulteta za varnostne vede, Ljubljana.
21. Lamberger, I. (2011). *Model zaščite elektronskih plačilnih sistemov pred zlorabami [doktorska disertacija]*. Ljubljana: Univerza v Ljubljani: Ekonomska fakulteta.
22. Liebowitz, M. (2011). *Romanian Hackers Charged in Subway Sandwich Card-Swipe Scheme*. Prevzeto 28. decembra 2011 iz http://www.securitynewsdaily.com/romanian-hackers-subway-sandwich-scheme-1409/
23. Maniam, B., in Earl, R. (2006). Perspectives on Credit Card Use and Abuse. *Journal of American Society of Business and Behavioral Sciences*, 2(1).
24. Mann, I. (2011). The turn of a Card. *Credit Management,* september 2011, 18–19.
25. Matyáš, V., Krhovják, J., Kumpost, M., in Cvrcek, D. (2008). Authorizing Card Payments with PINs. *Computer*, 41(2), 64–68.
26. Meško, G., Dobovšek, B., in Kešetović, Ž. (2009). Measuring organized crime in Slovenia. *Problems of Post-Communism*, 56(2), 58-62.
27. Montague, D. (2011). *Essentials of Online Payment Security and Fraud Prevention.* New Jersey: John Wiley & Sons, Inc.
28. *Payments fraud in Australia.* (2011). Prevzeto 10. februarja 2012 iz The Australian Payments Clearing Association (APCA): http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Media_Release_Payments_Fraud_Statistics_December_2011.pdf/$File/Media_Release_Payments_Fraud_Statistics_December_2011.pdf
29. *PCI DSS Compliance Trends Study, 2011.* (2011). Prevzeto 10. februarja 2012 iz iMPERVA: https://www.imperva.com/lg/lgw.asp?pid=440
30. *PCI DSS Trends 2010: QSA Insights Report.* (2010). Prevzeto 29. januarja 2012 iz Thales e-Security, Inc.: http://www.ponemon.

org/local/upload/fckjail/generalcontent/18/file/PCI%20DSS%20Trends%20-%20QSA%20Insights%20010310.pdf
31. *PCI Security Standards Council*. (2012). Prevzeto 11. januarja 2012 iz https://www.pcisecuritystandards.org/organization_info
32. *Pcistandard.com*. (2012). Prevzeto 11. januarja 2012 iz http://www.pcistandard.com/pci_standard.html
33. Pečar, J. (2002). Zmogljivost in uspešnost preprečevanja kriminalitete – nekaj dilem. *Revija za kriminalistiko in kriminologijo*, 54(4), 316–325.
34. Prabowo, Y. H. (2011). Building our defence against credit card fraud: a strategic view. *Journal of Money Laundering Control*, 14(4), 371–386.
35. *Predplacnik.si*. (2011). Prevzeto 29. januarja 2012 iz http://www.predplacnik.si/
36. Richards, M., Palmer, P., in Bogdanova, M. (2008). Irresponsible Lending? A Case Study of a U.K. Credit Industry Reform Initiative. *Journal of Business Ethics*, 81(3), 499–512.
37. Rizzardi, R. (2008). Financial Management – Payment Card Fraud Can Happen to You. *Optometry & Vision Development*, 39 (2), 64–65.
38. Segal, L., Ngugi, B., in Mana, J. (2011). Credit card fraud: a new perspective on tackling an intransigent problem. *Fordham Journal of Corporate & Financial Law*, 16, 743–781.
39. Sotlar, A. (2009) Post-conflict private policing : experiences from several former Yugoslav countries. *Policing*, 32(3), 489-507.
40. Stadler, W. A. (2012). Predatory lending: is The Credit CARD Act enough? *Journal of Financial Crime*, 19(1), 99–111.
41. Sullivan, R. J. (2010). *The changing nature of U.S. card payment fraud: industry and public policy options*. Prevzeto 5. maja 2011 iz Federal Reserve Bank of Kansas City: http://www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf
42. Tičar, B, Bohinc, R., in Nahtigal, M. (2010). Recepcija rimske antične vrednote fides - poštenosti in zvestobe dani besedi - v sodobnem slovenskem upravnem pravu. *Acta Histriae*, 18(4), 847-864.
43. Vellayan, N. (2011). PCI Compliance: What Your Franchise Should Know. *Franchising World,* november 2011, 20–22.
44. Whitmore, J. (2010). Safeguarding Cards. *Credit Union Management*, 33 (9), 24–26.
45. Wiese, B., in Omlin, C. (2009). Credit Card Transactions, Fraud Detection, and Machine Learning: Modelling Time with LSTM Recurrent Neural Networks. V M. A. Bianchini (ur.), *Innovations in Neural Information Paradigms and Applications* (str. 231–268). Springer Publishing Company.
46. Woolsey, B., in Gerson, E. S. (2009). *The history of credit cards*. Prevzeto 30. januarja 2012 iz CreditCards.com: http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php
47. Zakon o plačilnih storitvah in sistemih (ZPlaSS). *Uradni list RS 58/2009*.
48. Zupančič, M. (1999). Zlorabe plačilnih kartic pri elektronskem poslovanju. *Revija za kriminalistiko in kriminologijo*, 50(3), 215–224.

Payment cards fraud - card issuer's views

Igor Lamberger, Ph. D. in Economic Sciences, The General Police Directorate, Lecturer at Slovenian Police Academy and an external consultant (senior lecturer) at the Faculty of Criminal Justice and Security Studies, University of Maribor; e-mail: igor.lamberger@policija.si.

Bojan Dobovšek, Associate Professor and Vice-Dean of the Faculty of Criminal Justice and Security, University of Maribor, Slovenia; e-mail: Bojan.Dobovsek@fvv.uni-mb.si.

Boštjan Slak, postgraduate student at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia.

The purpose of this paper is to discuss some of the most common attributes, characteristics and assumptions that accompany payment card abuse (e.g. organised crime, key weaknesses in card security, usefulness of standards to ensure security, etc.), and then to empirically verify whether these assumptions hold in the eyes of employees who daily deal with the issue of payment cards and actually have the best insight into the topic. The first part consists of a literature review, and the second of statistically processed data we have obtained from a survey among personnel working in companies where payment cards are issued. A literature review and experience resulting from practice (both gave rise to the composition of a questionnaire) and then the empirical validation, showed that some attributes are true (international perpetrators, crime displacement, the magnetic stripe as a weak point). They also indicate that the role of repression is not as strong as many people would imagine. Due to the limited number of card issuers and the small number of people employed in this field, we have been confronted with difficulties in the implementation of more specific statistical analyses, since the ratio of the number of respondents to the number of variables proved to be quite restrictive. For further research, we suggest qualitative approaches (interviews or case analysis).

Key words: credit cards, payment cards, frauds, prevention, repression.

UDC: 343.37:343.85