UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

ZLORABA PLAČILNIH KARTIC NA BANČNIH AVTOMATIH IN POSTOPEK REŠEVANJA

Ljubljana, avgust 2013 GREGOR KAMBIČ

IZJAVA O AVTORSTVU

Spodaj podpisani Gregor Kambič, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor diplomskega dela z naslovom Zloraba plačilnih kartic na bančnih avtomatih in postopek reševanja, pripravljenega v sodelovanju s svetovalko prof. dr. Džonova Jerman Blažič Borka.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v diplomskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega diplomskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne_____ Podpis avtorja:_____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Hiter in nenehen razvoj je zgolj posledica in prilagoditev dejstvu, da živimo v času, ki narekuje hiter tempo življenja, hkrati pa je za nas tudi neke vrste vodilo, saj od nas zahteva hitro prilagajanje spremembam in njihovo sprejemanje. Hitremu razvoju smo priča tudi v bančnem poslovanju, ki bi ga lahko uvrstili v vsakdanjo obveznost, saj nas spremlja skoraj na vsakem koraku, pa naj si gre za enostaven nakup v trgovini ali pa za recimo nekoliko bolj zahteven nakup športnih copat prek spleta. Tako se bančno poslovanje vse bolj prilagaja uporabniku in usmerja k prihranku dragocenega časa. Ravno zato postajajo plačilne kartice vedno bolj priljubljeno plačilno sredstvo.

Hiter razvoj pa žal ne prinaša le prednosti, temveč tudi vedno več načinov zlorab, o katerih skoraj dnevno poročajo različni mediji. Uporabniki plačilnih kartic smo tako dnevno izpostavljeni različnim načinom zlorab, ki so iz dneva v dan bolj razvite in izpopolnjene. Prepoznavanje le-teh nam povzroča nemalo težav oziroma jih, kot splošni uporabniki plačilnih kartic, sploh ne prepoznamo. Največja slabost plačilnih kartic je zagotovo magnetni trak, ki ga nepridipravi z namestitvijo raznih naprav na bankomatih ali v trgovinah na POS terminalih (angl. *Point Of Sale*, v nadaljevanju POS) z lahkoto prestrežejo in preberejo magnetni zapis, kakor tudi osebno identifikacijsko številko - PIN (angl. *Personal Identification Number*). Dejstvo, da sta varnost in zaupnost med najpomembnejšimi elementi bančnega poslovanja ter ozaveščenost o slednjem pri strokovnjakih s kartičnega področja, je pripeljalo do razvoja pametne kartice, s katero se želi zagotoviti tako varnost in zaupanje, kot tudi enostavno uporabo in še večjo priljubljenost med uporabniki. In ravno uvedba pametne kartice z vgrajenim čipom, ki omogoča obsežnejšo hrambo podatkov, naj bi preprečila oziroma onemogočila zlorabe, vendar se moramo zavedati, da popolne varnosti pri uporabi plačilnega sredstva v obliki kartice skoraj zagotovo ni mogoče zagotoviti. Včasih imamo celo občutek, da so nepridipravi vedno korak pred strokovnjaki, ki skrbijo za razvoj varnosti kartičnega poslovanja.

Namen diplomskega dela je na podlagi pregledane literature raziskati in predstaviti zgodovino razvoja plačilnih kartic, razvoj glede na funkcionalnosti ter obdelati in predstaviti najbolj pogoste zlorabe, do katerih pride skoraj vsakodnevno.

Cilj diplomske naloge je obdelati postopke, ki jih izvaja banka X v primeru suma zlorabe plačilnih kartic in ravnanje bančnih uslužbencev v takšnih primerih. To je snemanje magnetnega zapisa na plačilnih karticah (angl. *skimming*) s pomočjo nestandardnih naprav, nameščenih na bančnem avtomatu ali POS terminalu. Cilj je tudi predstaviti statistične podatke o zlorabah skozi leta na banki X. Zaradi varstva poslovnih podatkov ime banke ne bo navedeno.

Prvi del diplomskega dela je namenjen teoretičnemu delu, kjer bo predstavljen zgodovinski razvoj plačilnih kartic, vrste plačilnih kartic po funkcionalnosti ter najpogostejše zlorabe plačilnih kartic. V drugem delu sledi predstavitev statističnih podatkov o zlorabah skozi leta na banki X, analizirana bo ponudba plačilnih kartic na slovenskem trgu, možnosti zavarovanja le-teh in cenovni vidik različnih postavk. Nato sledi obdelava postopkov, ki jih izvaja banka X v

primeru suma zlorabe plačilnih kartic. V zaključku diplomskega dela pa bodo navedeni bistveni preventivni ukrepi in priporočila bank, procesnega centra Bankart in Združenja bank Slovenije (v nadaljevanju ZBS) za preprečevanje oziroma zmanjševanje zlorab plačilnih kartic.

1 PLAČILNE KARTICE

Plačilne kartice so v današnji potrošniško naravnani družbi postale skoraj nepogrešljiv sopotnik vsakega posameznika, o svojih pravicah in obveznostih, povezanih z njihovo uporabo, pa se pogosto vprašamo šele, ko se sami soočimo s krajo ali izgubo plačilne kartice. Plačilna kartica sodi med elektronske plačilne instrumente, kjer je mogoče plačilo opraviti le s pomočjo elektronskih terminalov, prek katerih se nalog za plačilo v elektronskem omrežju posreduje do banke, pri kateri ima imetnik plačilne kartice deponirana oziroma odobrena denarna sredstva. Banka na podlagi prejetega naloga za plačilo opravi prenos denarnih sredstev na ciljni račun (Trstenjak, 2003, str 24-25).

Gradišar in Lamberger (2011, str. 15-16) pravita tako: »Brezgotovinsko poslovanje, ki ga omogočajo plačilne kartice, se je v sodobnem plačilnem prometu zelo razvilo in ponekod že presega gotovinsko plačevanje. Kreditne in plačilne kartice imenujemo tudi »plastičen denar«, saj se pojavljajo v obliki standardiziranih plastičnih kartic z magnetnim zapisom. Magnetni zapis vsebuje vse podatke o imetniku kartice, banki izdajateljici in možnosti plačevanja in dvigovanja gotovine na bančnih avtomatih. Prav magnetni zapis predstavlja eno od slabosti »plastičnega denarja«, saj zaradi nezadostne zaščite prihaja do raznovrstnih zlorab tega plačilnega inštrumenta.«

Dejstvo, da je z vidika varnosti najbolj sporen ravno magnetni zapis na plačilni kartici, je pripeljalo do razvoja kartic, ki vsebujejo tako magnetni zapis kot tudi elektronski čip. Že leta 2003 je Banka Koper izdala prvo tako imenovano pametno kartico, ki je vsebovala tudi elektronski čip. Konec leta 2004 je Banka Koper začela z redno izdajo pametnih kartic.

Logar (1998, str. 326) pravi takole: »V Sloveniji so plačilne kartice predvsem kreditne kartice, mednje pa uvrščamo kartice z odloženim plačilom in kartice, ki imetnikom omogočajo obnavljajoče se posojilo v višini odobrenega negativnega stanja na računu.«

Pri uporabi plačilnih kartic, ki so zagotovo eden od najbolj priljubljenih načinov plačevanja tako za fizične osebe kot podjetja, obstajajo obojestranske koristi, kar je tudi posledica vedno večje priljubljenosti, in sicer tako za imetnike, kot tudi za banke oziroma izdajatelje. Imetniki plačilnih kartic se izognejo dolgotrajnemu pisanju čekov, ne čutijo potrebe po tem, da morajo imeti v denarnici vedno veliko gotovine, dostop do denarja jim je prek bančnih avtomatov omogočen 24 ur na dan skozi vse leto tako doma kot v tujini, prav tako pa so nepogrešljive pri nakupih prek spleta, ki so v velikem porastu. Plačilne kartice za marsikoga predstavljajo tudi statusni simbol, saj poznamo različne vrste plačilnih kartic (zlate, črne, platinaste, itd., kar naj bi ponazarjalo finančno stanje imetnika). Banke kot izdajateljice vidijo svoje koristi predvsem z vidika pridobivanja provizij iz naslova plačila blaga in storitev, provizij za dvige gotovine in drugih

prihodkov (kot recimo kreditne obresti, članarine in ostalo), srečujejo se z lojalnostjo strank in možnostjo navzkrižne ponudbe, kot tudi z nižjimi stroški poslovanja v primerjavi z gotovino ali izdajanjem čekov.

1.1 ZGODOVINA PLAČILNIH KARTIC

Začetke plačilnih kartic v takšni obliki in uporabi je mogoče zaslediti že davnega leta 1950 v Združenih državah Amerike. Poslovnež Frank McNamara se je znašel v dokaj kočljivi situaciji, ko ni imel zadosti denarja za plačilo večerje v restavraciji, in v misli se mu je prikradla zamisel o plačilni/kreditni kartici. Vse skupaj se je začelo leta 1949, ko je Frank McNamara rezerviral poslovno večerjo v restavraciji Major's Cabin Grill. Po večerji, ko je natakar prinesel račun, je Frank segel po denarnici in neprijetno presenečen ugotovil, da je ta ostala v prejšnjem suknjiču. Iz zadrege ga je rešila žena, ki je prinesla denar, vendar ga je dogodek vznemiril do te mere, da se mu je porodila zamisel o uvedbi brezgotovinskega plačevanja.

Tako sta se februarja 1950, ne vedoč, da bosta popolnoma spremenila način plačevanja po celem svetu, Frank in njegov poslovni partner Ralph Schneider vrnila v isto restavracijo in naročila večerjo. Ko je natakar prinesel račun, se je Frank predstavil z majhno, kartonasto kartico - Diners Club Card in se podpisal na račun. Beseda Diners izhaja iz angleške besede dinner in v angleščini pomeni večerja. V industriji kreditnih kartic je ta dogodek znan kot »Prva večerja«. Diners Club se ja tako v zgodovino vpisal kot pionir na področju brezgotovinskega poslovanja.

Način brezgotovinskega plačevanja in plačila z zamikom se je kaj hitro uveljavil tako med potrošniki kot med trgovci, ki so na ta način bolje izkoristili nakupovalno moč svojih strank. Sredi 60. let prejšnjega stoletja je število plačilnih kartic predvsem po zaslugi MasterCarda, Eurocarda, Vise, American Expresa in Diners Cluba znatno naraslo. Rast pa se je v prihodnosti le še okrepila, kar potrjuje dejstvo, da smo danes, skozi različne kartične sheme, priča nekaj deset tisočim transakcijam na sekundo (Lešnik, 2012, str. 3-4).

Z vidika varnosti kartičnega poslovanja sta zagotovo pomembni letnici 1974 in 1994. Leta 1974 je francoski publicist Roland Moreno registriral patent samostojne elektronske naprave, ki vsebuje pomnilnik. Gre za kartice z integriranim vezjem, ki so bile kasneje poimenovane z vzdevkom pametne kartice (angl. *smart cards*). Leta 1994 pa so se trije največji svetovni izdajatelji kartic Europay/Eurocard, MasterCard in Visa (EMV) dogovorili za enoten nastop na področju uvajanja tehnologije pametnih kartic. Takrat je tudi izšla skupna EMV specifikacija, ki je namenjena razvoju bančnih čipnih kartic.

1.2 ZGODOVINA PLAČILNIH KARTIC V SLOVENIJI

Začetki razvoja plačilnih kartic v Sloveniji segajo v leto 1989, za kar je zaslužna Banka Koper (takratna Ljubljanska banka, Splošna banka Koper). Prvo domačo plačilno kartico je leta 1989 izdala delniška družba FIBA. Zaradi nesoglasij pri trženju plačilne kartice z delniško družbo FIBA se leta 1992 Banka Koper odloči za samostojno pot in tako marca 1992 nastane

samostojna blagovna znamka Activa in kartični sistem Activa. Sredi leta 1993 je bilo Activinih kartic že prek 50.000, prodajnih mest, ki so sprejemala to kartico pa prek 4.000. Že konec istega leta so se pripravljali na uvedbo POS terminalov.

24. 5. 1994 Banka Koper izvede prvo POS transakcijo, do konca leta pa jim uspe namestiti skoraj 100 POS terminalov. Istega leta sistem Activa prične z izdajo kombiniranih kartic Activa Eurocard/MasterCard. V prihodnjih letih je Banka Koper v sodelovanju s Poslovnim Sistemom Mercator d.d. razvila program zvestobe, ki sloni na plačilni kartici z vgrajenim pomnilniškim čipom, točke zvestobe pa se zapisujejo na kartico prek POS terminala ob vsaki transakciji. Sledi uvedba bančnih kartic Activa Maestro, kar omogoča dvigovanje gotovine v celotni mreži poštnih okenc v državi. Leta 1999 uvede elektronsko trgovino, ki omogoča plačevanje blaga in storitev prek spleta. Pričnejo se uporabljati prvi GSM (angl. *Global System for Mobile*) POS terminali. V letu 2000 je Banka Koper postala principalni član sistema Visa International; istega leta število kartic preseže število 700.000. Kmalu po uvedbi kreditne kartice Visa so uvedli tudi debetno kartico Visa Electron. Leta 2003 so izdali že milijonto Activino kartico ter prvo pametno plačilno kartico v Sloveniji. Poskusni skupini strank Banke Koper so izročili tudi prve čipne kartice Activa Maestro. Prva EMV transakcija na POS terminalu v Slovenji se je zgodila 21. 7. 2005. To je pomenilo tudi množični prehod na tehnologijo pametnih kartic EMV. Sistem Activa je pričel z zamenjavo vseh kartic z magnetno stezo s pametnimi karticami. V sistemu Activa je bilo takrat aktivnih več kot milijon kartic. Zamenjava kartic je za seboj potegnila tudi obvezno prilagajanje POS terminalov in bankomatov na standard EMV (Zgodovina pametnih kartic, 2013).

1.3 VRSTE PLAČILNIH KARTIC

Glede na to, da poznamo več vrst plačilnih kartic, je samoumevno tudi to, da jih lahko ločimo po različnih kriterijih. Na način plačila ločimo debetne, kreditne, kreditne z odloženim plačilom in predplačilne kartice. Na vrsto komitenta jih ločimo na klasične za občane, poslovne (kreditne in tudi debetne) in elitne (zlate, platinaste, črne, signia). Glede funkcionalnosti jih lahko ločimo na bančne in partnerske (kartice pripadnosti – angl. *affinity* kartice in partnerske kartice – angl. *co-brand* kartice). Nadalje bi jih lahko ločili tudi glede na izvor oziroma uporabnost, in sicer na tuje oziroma mednarodne kartice (uporabne so po vsem svetu), domače kartice (uporabne so samo v domači državi) ter licenčne (so lahko tako tuje kot domače, izdajatelj mora pridobiti ustrezne pravice za izdajanje).

Debetne kartice

»Debetna kartica, ki bi ji lahko rekli tudi plačilna ali obremenjevalna kartica, je prepoznavna kartica, ki omogoča plačilo s takojšnjim knjiženjem v breme njegovega imetnika; izraz obremenjevalna kartica izhaja iz dejstva, da njena uporaba povzroči knjižbo v breme, to je na debetni strani ustreznega računa v banki; razlikuje se od kartice zaupanja oziroma kreditne kartice.« (Turk, 2000, str 445).

Lamberger (2011, str. 44) pravi da: »Debetne kartice omogočajo imetnikom, da z njimi plačujejo blago in storitve. Pri nas so se pojavile v letu 1997, ko so banke klasični identifikacijski funkciji plastične kartice dodale možnost izvajanja plačil na elektronskih terminalih. Plačila za nakupe takoj po izvršeni transakciji ali neposredno po njej bremenijo imetnikov račun pri banki, ki je kartico izdala. Debetna kartica je kartica, ki jo dobimo v banki ob otvoritvi računa. Združuje dve funkciji. Gre za nadomestilo čekovne kartice, ki je služila potrjevanju čekov - identifikacijska funkcija, in dvigovanju gotovine na bančnih avtomatih - bankomatska funkcija. Debetna kartica nadomešča čeke, bankomatska funkcija pa ostaja enaka kot pri čekovni kartici. Novost debetne kartice v primerjavi s čekovno pa je predvsem v možnosti plačevanja na elektronsko opremljenih prodajnih mestih – POS terminali.«

V Sloveniji vsak imetnik osebnega računa prejme tudi debetno kartico. V veliki meri so to licenčne kartice mednarodnega kartičnega sistema MasterCard z oznako Maestro in Cirrus. Omogočata preprosto plačevanje blaga in storitev ter brezgotovinsko poslovanje z lastnim denarjem tako doma kot tudi v tujini. Kartici sta uporabni v tistih državah sveta na bankomatih in prodajnih mestih, ki so označena z nalepko Maestro ali Cirrus. Dvig je možen tudi na prodajnih mestih s POS terminali ter ustrezno oznako »gotovina«. Omenjeno storitev omogočajo tudi vse enote Pošte Slovenije, kar je v določenih situacijah zelo priročno. Slabost dvigov na Pošti Slovenije je zagotovo ta, da le-ti niso brezplačni. Imetnik debetne kartice lahko z njo posluje ozirom opravlja storitve le v okviru dovoljenih mesečnih in dnevnih limitov. Višina odobrenega limita je odvisna predvsem od višine rednih mesečnih prilivov ter bonitetne ocene stranke. Obstaja tudi možnost pridobitve izrednega limita, ki je načeloma višji od rednega limita, seveda ob ustrezni boniteti in finančnem stanju stranke. Debetna kartica v kombinaciji s PIN geslom imetniku omogoča opravljanje nakupov na prodajnih mestih, opremljenih s POS terminali, poslovanje z bančnimi avtomati, kot tudi elektronsko bančništvo ter storitve, ki jih banke nudijo na samem bančnem okencu.

Tabela 1: Število izdanih debetnih kartic v Sloveniji skozi leta

Leto	**1998**	**2000**	**2002**	**2004**	**2006**	**2008**	**2010**	**2012**
Število	775.032	1.392.379	1.707.668	2.310.190	2.412.485	2.626.982	2.742.470	2.534.069
Porast/upad*	0	617.347	315.289	602.522	102.295	214.497	115.488	-208.401

Legenda: * lastni izračun.

Vir: Banka Slovenije, Bilten, 2013, str. 43.

V tabeli št. 1 je prikazano število izdanih debetnih kartic v Sloveniji od leta 1998 pa do 2012. Iz tabele je razvidna rast izdanih kartic. Od leta 1998 pa do 2012 se je povečala za približno 3,27 krat. Magično mejo milijon izdanih kartic smo dosegli že »davnega« leta 2000, ko je bilo ob koncu leta izdanih 1.392.379 kartic. Iz tabele je razvidno, da število debetnih kartic vztrajno narašča, kar je posledica enostavnosti uporabe in vedno večje priljubljenosti med ljudmi.

Kreditne kartice

»Kreditna, ali kartica zaupanja ali priznavalna kartica je listina v obliki prepoznavne kartice, na podlagi katere lahko njen zakoniti imetnik kupuje blago oziroma uporablja storitev pri tistih podjetjih, ki so sklenila ustrezno pogodbo z njenim izdajateljem; kupljeno blago oziroma storitve plača kupec in zakoniti imetnik takšne kartice na podlagi izdajateljevega obvestila in računa oziroma se plačilo opravi s prenosom s tekočega računa ali žiro računa imetnika takšne kartice; izraz priznavalna kartica izhaja iz dejstva, da se na podlagi uporabe te kartice ustrezni račun v banki najprej prizna (to je knjiži na kreditni strani); razlikuje se od plačilne kartice.« (Turk, 2000, str 840).

»Kreditna kartica je plačilni inštrument in je po svoji naravi izkazni papir, saj se imetnik z njo izkaže pri prevzemu blaga ali storitve in z njo plača. Ob samem nakupu oziroma prevzemu blaga pa dejansko do plačila še ne pride, kajti imetnik kreditne kartice z njeno predložitvijo in podpisom oziroma vnosom osebne identifikacijske številke – PIN geslom, potrdi prevzem blaga, prodajalec pa mora račun izdati izdajatelju kreditne kartice. Ta plača račun prodajalcu in ga nato zaračuna imetniku kreditne kartice. Končno plača račun seveda imetnik kreditne kartice, to je kupec.« (Odar, 2000, str. 94).

Za kreditne kartice lahko rečemo, da je njihovo bistvo odloženo plačilo. To pomeni, da imetnik poravna račun za blago ali storitev, plačal pa ga bo šele čez nekaj časa. Tako nastane kreditno razmerje med imetnikom in izdajateljem kartice. Imetnik kartice dolg do izdajatelja poravna v skladu s pogodbenimi določili.

Poznamo tudi ***revolving*** **kreditno kartico** ali **kartico z odloženim plačilom**. Plačilna kartica z revolving funkcijo je kartica, s katero imetnik plačuje blago in storitve na prodajnih mestih in dviga gotovino ter obveznosti poravnava v več mesečnih obrokih. Pri omenjenih karticah se v tekočem mesecu plača le določen odstotek obveznosti ter pripadajoče obveznosti, preostanek pa se prenese v naslednji mesec. Del obveznosti se tako prenaša iz meseca v mesec. Pri kartici z odloženim plačilom imetnik svojo porabo plačuje z zamikom brez obresti, in sicer praviloma enkrat mesečno na določen dan, ki ga imetnik izbere na podlagi predlaganih dni s strani izdajatelja.

Vemo, da ima vsaka stvar svoje prednosti in slabosti, nič drugače pa ni niti s kreditno kartico. Prednost kreditne kartice za imetnika je zagotovo v njeni uporabnosti, saj lahko imetnik z njo plačuje in dviguje gotovino, kot to lahko počne z debetno kartico. Seveda je pri tem omejen z limitom ozirom zneskom odobrenega kredita na kartici, ki ga dobi na podlagi bonitetne sposobnosti ter rednih mesečnih prilivov. Velika prednost je tudi to, da omogoča plačevanja prek spleta. Ostale prednosti kreditne kartice so brezgotovinsko poslovanje, obrestovanje sredstev na računu, kljub plačilu blaga ali storitev, ki »ležijo« na banki do poravnave obveznosti, ter možnost uporabe tako doma kot v tujini na ogromno prodajnih mestih in bančnih avtomatih. Slabost kreditne kartice se kaj hitro opazi pri ljudeh, ki so zelo potrošniško naravnani. Ker gre za brezgotovinsko plačevanje, pogosto izgubijo občutek za svoje realne finančne zmožnosti in se z

nakupi nad svojimi zmožnostmi kmalu znajdejo v finančni stiski. Imetniki kreditnih kartic morajo vedeti, da strošek članarine ni ravno zanemarljiv ter se seveda zavedati tudi višjih provizij ob uporabi kreditne kartice z ostalimi vrstami plačilnih kartic. Zagotovo pa slabost predstavlja možnost zlorabe kartice ob nakupih prek spleta, ki jo lahko delno preprečimo z uporabo dodatnih varnostnih standardov, kot je recimo 3-D Secure. »3-D Secure je mednarodni varnostni standard, ki ga podpirata MasterCard (angl. *MasterCard SecureCode*) in Visa (angl. *Verified by Visa*) in se uporablja za preverjanje istovetnosti uporabnikov kartic pri spletnem plačevanju.« (Kaj je »3-D Secure«?, 2013).

Tabela 2: Število izdanih kreditnih kartic v Sloveniji skozi leta

Leto	**1998**	**2000**	**2002**	**2004**	**2006**	**2008**	**2010**	**2012**
Število	593.863	742.071	847.450	1.011.236	1.207.052	1.378.743	1.531.465	1.606.520
Porast/upad*	0	148.208	105.379	163.786	195.816	171.691	152.722	75.055

Legenda: * lastni izračun.

Vir: Banka Slovenije, Bilten, 2013, str. 43.

Vedno večja priljubljenost in uporaba kreditnih kartic je razvidna iz tabele št. 2, saj se število izdanih kreditnih kartic nenehno povečuje. Od leta 1998 do 2012 se je število izdanih kreditnih kartic povečalo za približno 2,71 krat.

Predplačilne kartice

Za predplačilno kartico (angl. *pre-paid card*) je značilno to, da se denar nanjo naloži že pred samo uporabo. Predplačilna kartica je enakega videza kot kreditna ali debetna kartica, to pa še ne pomeni, da ima tudi enako uporabnost. V primerjavi s kreditno kartico se razlikuje v tem, da ne omogoča kredita, ampak zgolj porabo pred tem naloženih sredstev. Bistven razkorak z debetno kartico pa predstavlja dejstvo, da se za njeno pridobitev ne zahteva osebnega računa, rednih mesečnih prilivov ali zaposlitve, posledično to pomeni, da lahko pride do porabe sredstev v višini, ki so bila predhodno naložena, in ne do prekoračitve stanja.

Obstajajo predplačilne kartice, ki so brezimenske in omogočajo samo enkratno nalaganje in uporabo pri točno določenih trgovcih (primer takšne kartice je recimo Darilna kartica Mercator, ki je uporabna v Mercatorju, M Tehniki, M Holidaysu, Modiani ter InterSportu). Obstajajo tudi brezimenske predplačilne kartice z enkratno naloženimi sredstvi in z možnostjo uporabe na vseh mestih z ustrezno oznako. Poznamo pa tudi personalizirano ali pametno predplačniško kartico, ki omogoča večkratno nalaganje sredstev ter uporabo po celem svetu.

Kartice zvestobe

Kartice zvestobe, rečemo jim tudi kartice ugodnosti ali lojalnosti, so vedno bolj razširjene in priljubljene. V šali bi lahko rekli, da ima vsak Slovenec v svoji denarnici vsaj eno kartico zvestobe. S karticami zvestobe so najprej začeli trgovci in drogerije, sedaj pa jih izdajajo tudi

manjše trgovine. Z njimi želijo izdajatelji nagraditi zaupanje in zvestobo svojih članov oziroma imetnikov ter jih na tak način tudi vedno znova zvabiti nazaj oziroma obdržati. In dandanes je težko ravno to – nekoga obdržati, zato smo priča vsakodnevnim medijskim vojnam vodilnih podjetij z oglasnimi sporočili, kjer reklamirajo tako posebne ponudbe kot tudi kartice zvestobe.

Kartice pripadnosti (angl. *affinity cards*)

So kartice, katerih dobičkonosnost ni v ospredju, ampak gre za povezovanje članov organizacije pri projektu skupne kartice, kjer imajo člani skupne cilje, vrednote, hobije in ostalo. Kartice pripadnosti izdajajo banke v povezavi z različnimi organizacijami, društvi, humanitarnimi in drugimi dobrodelnimi organizacijami. Bistven namen kartice je poistovetenje in pridobivanje članov.

Partnerske kartice (angl. *co-brand cards*)

Za razliko od kartice pripadnosti je skupni cilj partnerske kartice dobičkonosnost in maksimiranje koristi obeh partnerjev. Partnerske kartice izdajajo banke in podjetja z namenom pridobivanja novih članov, pospeševanja prodaje in uporabe kartice za oba partnerja, kar pomeni tudi večjo dobičkonosnost. Ob koriščenju partnerskih kartic imetniki prejmejo razne ugodnosti. Za partnersko kartico tako lahko trdimo, da imajo pri njej koristi vse tri strani. Izdajatelj pridobi nova prodajna mesta, poveča število uporabnikov in finančni promet, partner lahko z nadgradnjo kartice omogoča njeno uporabo po svetu ter se izogne težavam s plačili, saj to odgovornost prevzame izdajatelj kartice, imetnik kartice pa poleg raznih ugodnosti pridobi tudi možnost, da izkoristi prednosti kreditne kartice. Slabost predstavlja le nezdružljivost uporabe različnih partnerskih kartic, kar onemogoča seštevanje koristi oziroma ugodnosti pri različnih partnerjih.

1.4 FIZIČNE LASTNOSTI KARTICE TER UPORABLJENA TEHNOLOGIJA

Da lahko kartico uporabimo kjer koli na svetu, je bila potrebna standardizacija njenih fizičnih lastnosti. Pomanjkanje standardov v prvih letih razvoja se je odrazilo predvsem v nezdružljivosti kartic različnih proizvajalcev, kar je tudi močno omejilo njeno uporabo. To je bil razlog za sprejetje standardov, ki podrobno opisujejo lastnosti kartic in se jih morajo držati vsi proizvajalci.

Mere, vsebina, zaščitni varnostni elementi, mesto in vrsta zapisa podatkov ter podatkovni del - magnetni trak ali spominski čip so točno predpisani in standardizirani z ISO standardi 7810, 7811, 7812, 7813, 7816 in 4909 (Lamberger, 2011, str. 52).

Kartica je debeline 0,76 mm, dolžina kartice je 8,576 cm, širina 5,389 cm. Prečna stranica v vogalu med stranico dolžine in stranico širine meri 3,18 mm. Kartica na sprednji strani vsebuje logotip izdajatelja, številko kartice, veljavnost, podatke o imetniku in označbo vrste kartice. Na zadnji strani se nahaja magnetni trak, ki se začne na razdalji 0,592 mm od prečnice vogala kartice, CVC številka (angl. *card verification code*) in mesto za podpis imetnika. Jasno je, da sta

tako sprednja kot tudi zadnja stran kartice strogo predpisani in omejeni z namenom standardizacije uporabe in zagotavljanja enakosti izdanih kartic, kakor tudi ločevanja glede namembnosti kartice, njene uporabe in izdajatelja. V primeru pametnih kartic je na sprednji strani v levem delu nameščen čip oziroma spominsko-procesorski del kartice. Velikost čipa je s standardom omejena na 25 mm², velikost čipa pa je omejena tudi iz fizikalnega razloga, saj bi se ta lahko na sicer mehki kartici ob upogibanju poškodoval (Lamberger, 2011, str. 52-53).

Poznamo še veliko drugih pomembnih standardov, ki so bolj povezani s samim delovanjem kartic in kartičnega sistema in ne toliko s fizičnimi lastnostmi. Takšen je na primer EMV standard ali SET (angl. *Secure Electronic Transactions*), to je skupina standardov za plačila s kreditnimi karticami prek omrežja s številko kartice. SET so skupaj razvili CyberCash, GTE, IBM, MasterCard, Microsoft, Netscape in Visa.

S samega tehnološkega vidika pa bi lahko kartice razdelili na magnetne, pametne kartice (čipna tehnologija) ter laserske in virtualne.

Magnetne kartice

Značilnost magnetne kartice je magnetni trak, ki se po navadi nahaja na zadnji strani kartice in omogoča shranjevanje manjše količine bistvenih podatkov o imetniku ter izdajatelju. Tako zapisanim podatkom rečemo magnetni zapis. Magnetna kartica omogoča, da podatke z nje lahko le beremo, ne moremo pa jih spreminjati.

Z željo po hitrem in učinkovitem opravljanju storitev, kot so storitve na bančnih avtomatih in plačevanje prek POS terminalov, so jo razvili proti koncu 60. letih v podjetju IBM Information Records Division (International Business Machines Corporation). Magnetno snemanje na »jekleni« trak in žice za snemanje zvoka so izumili že med drugo svetovno vojno (Magnetic stripe card, b.l.).

Največjo slabost magnetne kartice predstavlja ravno magnetni trak, saj ga je mogoče prekopirati z ene kartice na drugo. In ravno zaradi velikega porasta zlorab v smislu snemanja magnetnega zapisa (angl. *skimming*) ter enostavnosti ponarejanja kartic, je prišlo do nadaljnjega razvoja kartic in uvajanja čipne tehnologije.

Pametne kartice (angl. *smart cards*)

Dejstvo, da sta varnost in zaupnost med najpomembnejšimi elementi bančnega poslovanja ter ozaveščenost o slednjem pri strokovnjakih s kartičnega področja, je pripeljalo do razvoja pametne kartice. Z njo se želi zagotoviti tako varnost in zaupanje, kot tudi enostavno vsestransko uporabo in še večjo priljubljenost med uporabniki.

Pametne kartice, ki jih poznamo tudi pod nazivi kartice z integriranim vezjem, kartice s čipom ali mikroprocesorske kartice, so kartice z vgrajenim mikročipom, ki omogočajo večjo

zmogljivost ter s tem celo vrsto dejavnosti in storitev. Lahko bi rekli tudi, da so pametne kartice v prvi vrsti »odgovor« na zlorabe magnetnih kartic, ki se jih da zlahka ponarediti in so pogosto tarče raznih kriminalnih združb, hkrati pa so rezultat vedno hitrejšega tehnološkega napredka in razvoja. Mikročip, ki je integriran v kartico, vsebuje vse pomembne podatke o imetniku v zvezi z identifikacijo, samim računom, dnevnim limitom in ostalim. Shranjeni so na bistveno bolj varen način kot pri magnetnih karticah. Mikročip s pomočjo procesorja nadzira vse interakcije, ki potekajo med kartico in zunanjimi napravami, ki posegajo (berejo in pišejo) na pomnilnik kartice. Enega izmed razlogov za prehod na pametne kartice lahko najdemo tudi v premajhni pomnilniški zmogljivosti magnetnega traku. Mikročip namreč omogoča shranjevanje bistveno več podatkov kot magnetni trak. Za pametne kartice lahko rečemo, da omogočajo preprostejše in cenejše poslovanje ter večjo varnost in združitev različnih tehnologij v eno.

Leti 1974 in 1994 sta s svetovnega in varnostnega vidika v povezavi s pametnimi karticami zelo pomembni. Že davnega leta 1974 je francoski publicist Roland Moreno registriral patent samostojne elektronske naprave, ki vsebuje pomnilnik. Leta 1994 pa so nov mejnik pri varnosti kartičnega poslovanja postavili trije največji svetovni izdajatelji kartic Europay/Eurocard, MasterCard in Visa (EMV), ki so se kljub veliki medsebojni konkurenčnosti na trgu dogovorili za enoten nastop na področju uvajanja tehnologije pametnih kartic. Takrat tudi izide skupna EMV specifikacija, ki je namenjena razvoju bančnih čipnih kartic.

V Sloveniji so to prelomnico naredili v Banki Koper leta 2003 s prvo izdajo pametnih kartic poskusni skupini njihovih strank. Po prvi uspešno izvedeni transakciji na POS terminalu so decembra 2004 začeli z redno izdajo pametnih kartic. Takrat so na Banki Koper kot prvi v Sloveniji prešli na tehnologijo pametnih kartic, ki upošteva obvezni mednarodni kartični sistem EMV. Pozneje so ji sledile tudi ostale banke in sedaj imamo v Sloveniji vse bančne kartice opremljene s čipom. Prehod na pametne kartice za bančni sistem ni bil poceni, saj je zahteval prilagoditev tako bančnih avtomatov kot POS terminalov, zamenjati pa je bilo potrebno tudi vse magnetne kartice.

Kljub vsem zgoraj omenjenim prednostim najdemo tudi slabosti pametnih kartic. Glavna slabost je zagotovo ta, da EMV standard ne velja po vsem svetu, zato imamo pametne kartice, ki imajo na hrbtni strani še vedno magnetni trak, kar omogoča njihovo uporabo tudi tam, kjer niso opremljeni s čipno tehnologijo. Naslednjo slabost uvedbe pametnih kartic lahko vidimo v zahtevi po visokih investicijah v nadgradnji bančnih avtomatov in POS terminalov ter seveda v celotni zamenjavi kartic, ki niso opremljene s čipom.

1.5 UPORABNOST PLAČILNIH KARTIC

Za plačilne kartice lahko rečemo, da so vedno bolj priljubljen instrument negotovinskega poslovanja. To dokazujeta tudi tabeli št. 1 in 2 v poglavju 1.3. V letu 2012 je bilo v Sloveniji skupaj izdanih 4.140.589 zgolj kreditnih in debetnih kartic. Če bi imeli podatek o vseh izdanih karticah (kartice zvestobe, partnerske kartice, zdravstvene kartice in ostale) bi bila ta številka zagotovo mnogo višja. Rast števila kartic je posledica dejstva, da se ljudje iz dneva v dan

zavedajo prednosti, ki jih nudijo, kot tudi tega, da se dokaj počasi, a vztrajno spreminjajo plačilne navade ljudi. In ravno nenehen razvoj, izboljšave ter nadgradnje, pa naj si gre za neko splošno področje ali področje plačilnih kartic, nam omogoča sledenje tempu, ki ga narekuje družba.

V Sloveniji opravimo v povprečju 51,3 kartičnih transakcij na leto, kar nas v Evropi uvršča v zgornjo polovico. Najmanj kartičnih transakcij na prebivalca opravijo v Grčiji (6,5), največ pa na Finskem (153,6) (Lešnik, 2012, str 15).

Bančni avtomati

Za bančne avtomate, ki so samopostrežni terminali, je značilno, da so povezani s centralnim računalnikom, kar nam omogoča, da brez prisotnosti bančnika opravljamo osnovne bančne storitve, kot so dvigovanje gotovine, izpis stanja, polog gotovine in ostalo. Zaradi tega jih tudi uvrščamo med samopostrežno bančništvo.

Razlog za nastanek bančnih avtomatov lahko iščemo v tem, da so se v poznih 60. letih zaradi družbeno ekonomskih potreb odločili banke ob sobotah zapreti, istočasno pa so želeli zagotoviti nemoten dostop do gotovine. Prvi bankomat je bil postavljen v Londonu že leta 1967. Omogočal je izplačilo po 10 funtov. V zameno za dvignjen denar je bil vložen kupon, le-ta je ostal avtomatu kot dokazilo o dvigu. Prvi bankomati so bili namenjeni dvigovanju gotovine, kasnejši razvoj pa je prinesel oziroma prinaša vedno nove funkcije. Poleg razvoja ustrezne tehnologije je bilo na začetku potrebno poskrbeti, da so ljudje bančne avtomate tudi sprejeli, in sicer tako uslužbenci bank (ki so v njih videli konkurenco) kot tudi same stranke. Slabosti prve generacije bančnih avtomatov so se kazale v tem, da bankomati niso uspeli ločiti med veljavnim, ukradenim ali izgubljenim kuponom ter niso bili povezani z bančnimi računalniki. Tako so leta 1972 v Lloyds Bank v Angliji postavili prvi bankomat, ki je bil povezan s centralnim bančnim računalnikom. Omenjeni bankomat je ob uporabi kartice z magnetnim zapisom uspel identificirati uporabnikov račun. Na Japonskem so šli v približno enakem obdobju še korak dlje, saj so razvijali bankomate, ki so omogočali več storitev kot le dvig gotovine.

V Sloveniji so leta 1990 prvi bankomat postavili v takratni Ljubljanski banki. Seveda je tudi pri nas konkurenca med bankami poskrbela za hiter razvoj in število bankomatov, kar je razvidno iz tabele št. 3.

Tabela 3: Število bančnih avtomatov v Sloveniji

Leto	**1998**	**2000**	**2002**	**2004**	**2006**	**2008**	**2010**	**2012**
Število	612	865	1.095	1.389	1.522	1.731	1.814	1.789

Vir: Banka Slovenije, Bilten, 2013, str. 44.

Bančni avtomat je sestavljen iz strojne in programske opreme. Osrednji del je klasični osebni računalnik, povezan z zaslonom, tipkovnico, tiskalnikom, čitalcem kartic, omrežno kartico,

podajalnikom denarja in depozitno enoto. Sestavni del bankomata je tudi sef, v katerem je shranjena gotovina ter kasetne enote.

Bistvene prednosti bančnih avtomatov vidimo v prihranku časa, 24-urni dostopnosti, v varnosti (recimo odvzem kartice, če več kot 3-krat zapored vnesemo napačno PIN številko ali pa če je kartica fizično poškodovana oziroma razmagnetena), enostavnosti uporabe (s pomočjo izpisa na zaslonu nas bankomat sam vodi skozi storitev oziroma postopek), raznovrstnosti storitev, ki jih omogočajo, ter v vedno novih odkritjih in možnostih. Slabosti pa se po drugi strani razkrivajo v tem, da vseh storitev ni možno opraviti na vseh bankomatih, banke zaračunavajo določene provizije ob uporabi le-teh, lahko pride do tehničnih težav (izpad električne energije, mehanska poškodba bankomata, izpad transporta gotovine in ostalo) in kaznivih dejanj (vandalizem in poškodovanje bankomata, sabotaža, vlom, rop pred bankomatom in ostalo).

Tabela 4: Število bančnih avtomatov na mio prebivalcev

Država	**Leto 2002**	**Leto 2012**
Nemčija	612	1.058
Francija	632	869
Italija	694	852
Nizozemska	466	477
Avstrija	870	906
Slovenija	551	905
Finska	794	530

Vir: B. Bertoncelj, Tveganje pri poslovanju z bančnim avtomatom, 2013, str. 4.

Iz tabele št. 4 je razvidno, da smo imeli leta 2002 v Sloveniji 551 bančnih avtomatov na milijon prebivalcev, leta 2012 pa že 905. To dokazuje, da imamo v Sloveniji, v primerjavi z državami navedeni v tabeli, dobro pokritost z bančnimi avtomati na milijon prebivalcev.

POS terminal

POS terminal je elektronska naprava, ki zaradi povezanosti z bančnim računalniškim omrežjem prek telefonske, internetne ali GSM povezave, omogoča elektronsko odčitavanje plačilnih kartic. Bistvo POS tehnologije je avtomatski prenos podatkov prek terminalov do računalnika v banki. POS terminali se nahajajo na prodajnih mestih in v plačilo sprejemajo plačilne kartice. Njihove glavne funkcije so posredovanje podatkov o višini zneska plačila v banko, preverba zavrnitve plačila s strani banke, preverjanje ustreznosti oziroma pravilnosti vnesenega PIN gesla ter s tem identifikacija uporabnika kartice in seveda tiskanje potrdila o plačilu.

Za uporabo POS terminala mora biti med trgovcem oziroma med imetnikom POS terminala in lastnikom oziroma izdajateljem sklenjena pogodba, v kateri se doreče podrobnosti, kot so mesečna najemnina, postavitev terminala, servisiranje, plačila provizij od prometa, ki se jih morata držati obe strani. Kako deluje plačilo preko POS terminala? Zelo na kratko lahko rečemo,

da se po vložitvi plačilne kartice v POS terminal vzpostavi on-line povezava z računalnikom izdajatelja kartice, sledi vnos PIN gesla, nato pa se opravi avtorizacija imetnika kartice. Ko banka izdajateljica kartice potrdi, da ima imetnik dovolj denarnih sredstev za plačilo ter da ni drugih ovir za plačilo (blokacija kartice), se plačilo odobri in plačniku se natisne potrdilo o plačilu prek POS terminala ter izda račun.

Prvo POS transakcijo v Sloveniji je 24. 5. 1994 izvedla Banka Koper. Do konca leta 1994 jim je uspelo namestiti skoraj 100 POS terminalov. Sledilo je bliskovito nameščanje POS terminalov, kar prikazuje tabela št. 5. Vedno večje število POS terminalov se odraža tudi v vedno večjem številu transakcij preko POS terminalov. Leta 2012 smo imeli v Sloveniji nameščenih 38.664 POS terminalov, prek katerih smo opravili 148.513.000 transakcij (Bilten BS, 2013).

Tabela 5: Število POS terminalov in transakcij prek POS terminalov (v tisočih) v Sloveniji

Leto	**1998**	**2000**	**2002**	**2004**	**2006**	**2008**	**2010**	**2012**
Št. POS terminalov	11.361	21.723	29.452	34.770	29.234	33.490	32.021	38.664
Št. transakcij prek POS v tisočih	…	49.376	91.750	110.771	115.367	134.581	138.853	148.513

Vir: Banka Slovenije, Bilten, 2013, str. 44.

Bistvene prednosti, ki jih prinaša POS tehnologija:

- avtomatska kontrola veljavnosti kartice,
- avtomatska avtorizacija,
- hitrost, varnost in enostavnost nakupa (v kolikor ni težav z vzpostavitvijo on-line povezave),
- potrdilo o nakupu se natisne samodejno,
- POS terminali omogočajo uporabo različnih kartic (ki odgovarjajo predpisanim standardom),
- enostavnost zaključka poslovanja,
- nižji stroški poslovanja z gotovino (ni tveganja pri prevzemu in oddaji gotovine),
- omogočanje dviga gotovine (na posebej označenih prodajnih mestih),
- raznolikost samih naprav (lahko so stacionarne, mobilne, majhne ali vgrajene skupaj z monitorjem na blagajni) in
- 24-urna strokovna pomoči s strani izdajateljev in procesnega centra.

2 ZLORABE PLAČILNIH KARTIC

V bančništvu smo priča hitremu, za nekatere uporabnike osnovnih bančnih storitev celo prehitremu, razvoju. Skoraj vsak dan lahko v medijih zasledimo razne novosti, ki jih banke ponujajo svojim komitentom, kar je odraz hude konkurenčne tekme za vsako stranko kot tudi dejstva, da želijo banke zadostiti ne samo zakonodaji in predpisom oziroma priporočilom, ampak tudi željam svojih komitentov. Nič drugače ni niti s plačilnimi karticami, ki so zaradi svoje priročnosti in enostavnosti uporabe vedno bolj priljubljene in uporabljane.

Veliko slabost plačilnih kartic vsekakor predstavlja dejstvo, da obstaja veliko možnih načinov zlorab. In ravno zaradi tega se vsi sodelujoči v kartičnem poslovanju zavedajo dejstva, da je varnost poslovanja s plačilnimi karticami ključnega pomena. Kljub vsem vloženim naporom s strani izdajateljev in organov zakona pa lahko na žalost rečemo, da so storilci vedno korak pred zakonom in tehnološkim napredkom, saj se zelo hitro prilagajajo spremembam in uvedenim novostim glede varnosti poslovanja s karticami.

2.1 VRSTE ZLORAB PLAČILNIH KARTIC

Zlorabe plačilnih kartic lahko razvrstimo v naslednje skupine:

- zlorabe s strani imetnika; do česar pride, ko imetnik kartice zavestno presega dovoljeno negativno stanje,
- zlorabe izgubljene ali ukradene kartice; tukaj gre za klasično kriminaliteto, in sicer lahko kriminalci na podlagi ropa, tatvine ali vloma pridejo do kartic, ki so potem kaj hitro tudi predmet zlorabe in
- zlorabe s ponarejenimi karticami; kriminalci s pomočjo raznih naprav kopirajo podatke s kartic in jih ponaredijo ter jih potem nemoteno uporabljajo (do odkritja zlorabe s strani imetnika oziroma izdajatelja kartice).

Gradišar in Lamberger (2011, str. 16), ugotavljata, da poznamo veliko načinov, kako priti do potrebnih podatkov, ki omogočajo zlorabo kartice, in veliko načinov zlorab:

- **prenarejanje kartic**,
- **ponarejanje kartic** (s pomočjo snemanja magnetnega traka),
- **pogled čez ramo ali »Libanonska zanka«**,
- **zlorabe bančnih avtomatov**,
- **trojanski konj ali lažni bankomat**,
- **zamenjava plastike** (Pri tej zlorabi so žrtve predvsem starejši ljudje. Ko opravljajo dvig na bankomatu, jih zmoti skupina storilcev, večinoma s kakšnimi vprašanji po naslovu, in ko se imetnik obrne stran od bankomata, mu ukradejo kartico. Ko imetnik opazi, da kartice ni, mu rečejo, da mu jo je »požrl« bankomat, ter da naj še enkrat vnese PIN številko, ki si jo seveda zapomnijo. Ko imetnik odide, misleč, da mu je bankomat res zadržal kartico, opravijo dvig ter imetnika oškodujejo.),
- **zlorabe kartic s strani trgovcev** (angl. *Merchant Fraud*) (Poleg skimminga na POS terminalih lahko rečemo, da prihaja s strani skorumpiranih trgovcev tudi do ostalih zlorab. Podatke o opravljeni transakciji lahko ponaredijo tako, da povišajo znesek, ali storilcem posredujejo zbrane podatke o svojih kupcih, ali v plačilo zavedno sprejmejo ponarejene ali izgubljene kartice.),
- **zloraba nikoli prejetih kartic** (Storilci v tem primeru ali ukradejo pošto, ali pa se povežejo s skorumpiranimi bančnimi uslužbenci. Teh zlorab je zelo malo že zaradi dejstva, da se PIN številka in kartica nikoli ne pošiljata skupaj ampak ločeno. Tudi če je kartica dejansko ukradena, imetnik to zelo hitro opazi.),

- **lažne prošnje za izdajo kartic** (Storilci z namenom pridobitve kartice in z zlorabo osebnih podatkov imetnikov kartic podajo lažno prošnjo za ponovno izdajo že izdane kartice. V večini primerov gre za spremembo naslova ali kaj podobnega. Te prevare so prava redkost, oziroma so zaradi postopkov pri izdaji novih kartic skoraj nemogoče, saj se takšni podatki preverjajo.),
- **zlorabe na podlagi pridobljenih potrdil o nakupu ali dvigu** (Včasih se je na potrdilih o nakupu ali dvigu nahajalo veliko pomembnih podatkov, ki so jih storilci uporabili za zlorabo kartice, in sicer na način, da so lastnika telefonsko nagovorili za preostale podatke ob pretvezi, da kličejo iz banke, ter da preverjajo zlorabo in potrebujejo številko kartice. Ko so jo pridobili, jim je bilo omogočeno plačevanje prek spleta. Danes potrdila ne vsebujejo toliko pomembnih podatkov, vendar do zlorab občasno še vedno prihaja pri naivnih uporabnikih.),
- ***Phishing* – ribarjenje** (V kartičnem poslovanju nezakonit način zavajanja uporabnikov z namenom pridobivanja tujih občutljivih osebnih podatkov oziroma kraje identitete. Pri takšnem zavajanju poskuša oseba, ki to izvaja, pridobiti podatke, npr. številke kreditnih kartic, gesla, podatke o računih ali druge osebne podatke tako, da pod pretvezo prepriča žrtev o potrebi po posredovanju teh podatkov.),
- ***Pharming* – zvabljanje** (Gre za podoben način zlorabe kot ribarjenje, s to razliko, da je nekoliko preoblikovano oziroma modificirano. Obstaja zvabljanje z napadi na internetne domenske ali DNS strežnike (angl. *Domain Name System*) in zvabljanje z napadi na datoteko o gostiteljih (angl. *hosts file*), ki se nahaja na računalniku uporabnika.).

Prenarejanje kartic

Prenarejanja kartic se storilci poslužujejo oziroma izvajajo v primerih, ko imajo v posesti prave kartice. Na pravi kartici, do katere pridejo ali s tatvino ali z najdbo izgubljene kartice, spremenijo podatke.

Storilci poskušajo na pravih karticah večinoma spremeniti fizični zapis na kartici, kot so ime, priimek ali identifikacijska številka kartice ali pa kar kombinacijo naštetega. Storilcem je lažje na kartico dodati recimo dodatno črko in tako spremeniti ime ali priimek (primer: moškemu imenu Žan na kartici dodajo črko a in dobijo žensko ime Žana), vendar pa tak način ni najboljši, saj se ukradene kartice hitro znajdejo na »stop listi«, s čimer je onemogočena njihova uporaba. Za storilce je zagotovo boljše, če spremenijo številko kartice - tako imajo več možnosti, da njihove kartice ne bo na »stop listi«, in lahko jo bodo nemoteno uporabljali. Po drugi strani pa je sprememba številke težje izvedljiva, saj je število številk na kartici vedno enako, kar pomeni, da morajo storilci s toplotnim posegom eno številko najprej odstraniti in nato dodati novo. Zaradi uporabe raznih kemikalij, ki so danes dostopne vsakomur, so za storilce zgoraj omenjene možnosti dokaj enostaven in cenovno ugoden postopek. Prenarejene kartice so zelo dobre, zato jih trgovci tudi težje prepoznajo.

Druga vrsta prenarejanja je spreminjanje magnetnega zapisa na kartici. Po uvedbi kartičnih kod, ki so po posebnem algoritmu izračunane številke (zajemajo podatke o izdajatelju, številki

kartice, imetniku in drugo), imajo storilci težave oziroma tega ne morejo narediti, če ne poznajo kode ali algoritma. Dodatno težavo storilcem predstavlja dejstvo, da je možno takšne kartice uporabljati samo na POS terminalih, kjer ni potrebno vnesti PIN gesla, temveč zadostuje podpis. Ob plačilu pa se lahko podatki na kartici preverijo s tistimi na izpisu in hitro pride do odkritja, da je kartica prenarejena.

Poglavitna prednost ukradenih kartic je zagotovo ta, da imetnik kartice kmalu opazi, da mu je bila kartica odtujena ali da jo je izgubil, ter jo lahko hitro prekliče. S preklicem se kartica uvrsti na »stop listo«. Prednost predstavlja tudi čipna tehnologija (upoštevanje EMV standarda) tako pri samih karticah kot pri POS terminalih in bančnih avtomatih. To pomeni, da storilci ne morejo opraviti nakupov brez ustreznega PIN gesla. Do težav prihaja v državah, ki še niso sprejele EMV standarda, saj kartice tam še vedno delujejo na podlagi magnetnega zapisa.

Ponarejanje kartic

Pri ponarejanju kartic storilci v celoti ponaredijo kartico. Tako obstajata dve identični kartici, ki ju posedujeta imetnik in ponarejevalec. Imetnik kartice uporablja svojo originalno kartico, nevedoč, da obstaja kopija njegove kartice, ki jo uporablja ponarejevalec. Zloraba takšne kartice traja vse do trenutka, ko imetnik originalne kartice opazi, da se njegov transakcijski račun bremeni tudi za zneske nakupov ali dvigov, ki jih sam ni nikoli opravil. V praksi to lahko pomeni tudi cel mesec, dokler oškodovanec ne prejme izpiska o poslovanju prek transakcijskega računa. V najboljšem primeru oškodovanec to opazi že prej prek elektronske banke ali pa to opazijo celo na procesnem centru, predvsem v primerih, ko gre za enormno povečanje uporabe kartice ali za uporabo v tujini, kar je še bolj sumljivo. Po odkritju se takšno kartico takoj blokira, kar onemogoči njeno nadaljnjo uporabo.

Lamberger (2011, str. 65) pravi tako: »Ponarejanje kartic poteka skozi več faz. Najprej je potrebno pridobiti osnovne materiale za izdelavo kartic, kot so plastika, magnetni trak in hologram. V svetu obstajata dve podjetji za izdelavo hologramov, več pa je ilegalnih, pri katerih je za hologram potrebno odšteti od 5 do 15 dolarjev. Prvi problem pri izdelavi kartice je vstavljanje hologramа. Hologram ne sme biti na površini kartice, ne sme se ga čutiti s prsti, zato je slabo ponarejene kartice lahko prepoznati. Lažja je izdelava magnetnega traku, v katerega vtisnejo izmišljene podatke (ime in priimek, številko računa, višino limita, idr.).«

Za ponarejanje kartice si morajo storilci zagotoviti vse potrebne podatke o kartici. To storijo tako, da z originalne kartice kopirajo fizični in magnetni zapis. Takšnemu kopiranju oziroma snemanju magnetnega zapisa po angleško rečemo skimming. Skimming se najpogosteje izvaja prek POS terminalov in bančnih avtomatov. Seveda pa ne gre zanemariti niti vdorov v sisteme kartičnih procesnih centrov ali spletnih trgovcev, kjer se ravno tako hranijo vsi potrebni podatki za ponarejanje kartic.

Do kopiranih magnetnih zapisov pridejo storilci s pomočjo različnih skimming naprav oziroma naprav, ki posnamejo kartične podatke in so narejene bodisi za zlorabe na POS terminalih ter

bančnih avtomatih ali kot samostojne enote (večinoma v gostinstvu, oziroma na tistih mestih, kjer uporabljajo prenosne POS terminale: natakar ima lahko poleg prenosnega POS terminala pri sebi še prenosno skimming napravo (kar prikazuje Priloga 1), skozi katero brez vednosti imetnika povleče kartico, po možnosti pa opazuje imetnika pri vnosu PIN gesla na POS terminal).

Za »popoln« skimming, ki storilcem omogoča nadaljnjo ponaredbo kartice, mora skimming naprava zajeti dve vrsti podatkov, to je magnetni zapis kartice ter seveda PIN številko. Tako pridobljeni podatki storilcem omogočajo ponaredbo in prosto uporabo takšne kartice. Da pa bi storilci lahko pridobili omenjen podatek, so skimming naprave večinoma narejene iz dveh delov. Prvi del omogoča zajem podatkov z magnetnega zapisa kartice. Gre za predelavo prenosnih čitalcev magnetnih kartic z vgrajenim pomnilnikom. Glede na to, da morajo takšni čitalci prebrati magnetni zapis kartice, morajo biti postavljeni v bližini reže ali kar na originalni reži za vstavljanje kartice. Seveda so skoraj identični originalni reži, zaradi česar jih zelo težko odkrijemo. Magnetni senzor, ki prebere zapis na kartici, je vgrajen na notranji strani plastike in je neopazen (razvidno iz Priloge 3). Drugi del naprave pa omogoča vizualni zajem PIN številk ob vnosu na bančnem avtomatu. V večini primerov so to predelane videokamere, ki so zelo majhne (Priloga 2, Slika 3) in so na bankomat nameščene tako, da zajamejo številčnico za vnos PIN številke in sam vnos tudi posnamejo. Pridobivanje PIN številke je možno tudi z namestitvijo lažne tipkovnice na bankomatu (Priloga 2, Slika 4). Lažna tipkovnica vsebuje spominsko vezje, ki omogoča shranjevanje vnesenih PIN gesel. Oba dela vsebujeta vgrajene Li-Ion baterije, kar jima omogoča avtonomno delovanje. Pridobljene podatke shranjujeta na »flash spominu«. Ker gre po navadi za veliko maso zajetih podatkov z različnih kartic, imata oba sistema vgrajen tudi časovnik, ki pozneje omogoča enostavno uskladitev pravilne PIN številke s pripadajočim magnetnim zapisom. Omenjene skimming naprave imajo možnost brezžičnega prenosa podatkov, zato so na bančnem avtomatu nameščeni oddajniki, v njihovi bližini pa sprejemniki skupaj s spominsko enoto (takšne naprave so našli nameščene v avtomobilih, na kolesu in ostalih napravah). Prenos zbranih podatkov pa lahko opravijo tudi na klasičen način, in sicer tako, da naprave, ki morajo biti predhodno odstranjene z bančnega avtomata, povežejo z računalnikom.

V sklop ponarejanja kartic bi lahko uvrstili tudi tako imenovano »belo plastiko« (angl. *White Plastic*). Gre za belo kartico, ki ne vsebuje razpoznavnih znakov (logotipov) izdajateljev, je brez naziva in brez številke kartice. Zaradi omenjenih razlogov se jo zlahka odkrije in jo je nemogoče uporabiti pri poštenih trgovcih, zato se velikokrat zgodi, da so trgovci za sprejem takšne kartice podkupljeni. Takšne kartice vsebujejo pravilen magnetni zapis in se najpogosteje uporabijo prek POS terminalov pri skorumpiranih trgovcih. Uporaba na bančnih avtomatih je nekoliko težja, večinoma zaradi nepoznavanja ustrezne PIN številke.

Pogled čez ramo ali »Libanonska zanka«

Temeljni značilnosti zlorabe »Libanonske zanke« sta nelegalno nameščen vložek v reži za vstavljanje kartice in pridobitev ustreznega PIN gesla kartice. Da storilci lahko pridejo do kartice, morajo v režo bankomata najprej vstaviti trak (imenujemo ga Libanonska zanka), ki

kartico zadrži in je ne spusti v bankomat, niti je ne vrne imetniku. Obstajajo pa tudi načini za vstavljanje plastičnega vložka pri reži za čitalnik kartice, ki bankomatu prepreči, da bi kartico vrnil lastniku. Sledi pridobitev ustrezne PIN številke, ki se lahko pridobi na več načinov. Storilci na bankomat nalepijo obvestilo o težavah bankomata z vračilom kartice ter da je zato potrebno večkrat vnesti PIN številko. V tem primeru stojijo zelo blizu bankomata, da lahko vidijo vnos PIN številke. Lahko se tudi prijazno ponudijo za pomoč (z raznimi zgodbami, da so imeli tudi sami podobne težave, pa jim je uspelo), nakar jim lastniki zaupajo PIN številko. Na obvestilu je tudi navedeno, da naj se zglasijo v svoji banki, če bankomat kartice ne vrne. Ko imetnik zapusti bankomat, storilec odstrani oviro na reži bankomata in si prilasti kartico ter z njo opravi dvig in tako oškoduje imetnika kartice. Prednost takšne zlorabe je v tem, da imetniki kartice kaj hitro sporočijo banki ali procesnemu centru, da jim je bankomat kartico zadržal, tam pa kartico nemudoma blokirajo in s tem onemogočijo njeno nadaljnjo uporabo. Imetnik je po navadi oškodovan za razpoložljivo stanje oziroma za višino dnevnega limita na kartici.

Zlorabe bančnih avtomatov

Najpogostejša oblika zlorab na bankomatih so nastavljene skimming naprave. Obstaja pa še nekaj drugih vrst zlorab, ki so povezane z bankomati.

Past za gotovino (angl. *cash trapping*) zagotovo sodi med takšne zlorabe. Pri tej zlorabi storilci z namestitvijo posebne letve na režo za izdajanje gotovine (Priloga 4), premazane z lepilom, bankomatu onemogočijo izdajo gotovine, saj se denar zagozdi v reži. Glede na to, da dvig poteka normalno, bankomat uporabnika pozove k dvigu denarja, na bančni strežnik pa ne javi napake, ker zaključi, da pri izplačilu do nje sploh ni prišlo, oziroma je ne zazna. Na drugi strani pa uporabnik seveda zapusti bankomat, misleč, da gre za tehnično napako. V tistem trenutku pride storilec, ki se nahaja v bližini, oviro odstrani in vzame denar.

Storilci bančni avtomat zlorabijo tudi tako, da na bankomatu opravijo najvišji možni dvig, in ko bankomat denar iz sefa pošlje v žleb ter se odpre loputa za izstavitev denarja, prekrijejo senzor na njej. Senzor na loputi zaznava izplačilo gotovine in ker je ta prekrit, bankomat na bančni strežnik sporoči napako ter stornira transakcijo. Storilec zatem odvzame gotovino, ne da bi se transakcija zabeležila na transakcijskem računu, oziroma znižala razpoložljivo stanje. Takšno dejanje imenujemo **napad na žleb bankomata** in se lahko ponavlja. Če storilec naredi zlorabo z lastno kartico, se ga kaj hitro odkrije, zato se večinoma poslužujejo ponarejenih kartic.

Pri zlorabi **bančnega avtomata s predalom** storilec opravi dvig manjšega zneska. Ko se loputa odpre, v njej pusti en bankovec. Storilec nato s ponovnim dvigom, tokrat z mnogo višjim zneskom (ali celo najvišjim možnim) nadaljuje, in ko bankomat denar pošlje v predal, zazna, da je v njem ostala gotovina od prejšnjega dviga, zato stornira dvig, ob tem pa storilec odpre loputo in vzame denar. Tudi to dejanje se lahko ponavlja.

Poznamo tudi zlorabo **bančnega avtomata z režo**. Storilec opravi najvišji možni dvig, nato ob izplačilu iz reže za izstavitev gotovine vzame samo sredinske bankovce. Glede na to, da je del

bankovcev ostal v reži, bankomat zazna napako ter jo sporoči na bančni strežnik. Sledi storno transakcije. Tudi v tem primeru lahko storilec svoje dejanje ponavlja. Z vidika skimminga ter zlorab na bankomatih bi lahko izpostavili še eno zlorabo, to je namestitev **lažnih bankomatov**. Storilci z namenom pridobivanja podatkov ter s tem ponarejanja kartic na frekvenčnih lokacijah postavijo lažne bankomate. Zaradi premišljene izbire pri postavitvi se ljudje sploh ne zavedajo, da je lažni bankomat postavljen na novo in ga v želji in potrebi po dvigu gotovine tudi uporabljajo. Ker gre za lažni bankomat, do izplačila sploh ne pride, ampak se na bankomatu izpiše obvestilo, da je v okvari. Na takšen način storilci pridejo do vseh potrebnih podatkov (do magnetnega zapisa in PIN številke).

2.2 STATISTIČNI PODATKI O ZLORABAH PLAČILNIH KARTIC

Za pridobitev statističnih podatkov o zlorabah plačilnih kartic lahko rečemo le to, da je pridobitev skoraj nemogoča. Pri pridobivanju se srečujemo tako s pomanjkljivimi podatki (nepopolne evidence in neenake definicije pri tipih zlorab ter s tem nezmožnost druženja podatkov) kot tudi s tem, da predvsem banke in licenčni imetniki ne želijo razkriti podatkov o zlorabah. Razlog lahko poiščemo predvsem v želji po tajnosti poslovanja in podatkov, ker ne želijo škoditi svojemu ugledu, v zakonskih omejitvah, ter v prikrivanju pred konkurenco.

Kljub posredovanju prošenj na procesni center Bankart d. o. o. in na ZBS, nam žal niso posredovali podatkov. S strani Bankarta smo prejeli odgovor, da kot procesni center ne morejo posredovati podatkov, ki so v lasti bank. S strani ZBS pa so nam sporočili, da omenjenih podatkov ne vodijo. V nadaljevanju bomo posredovali podatke, ki jih v svojih letnih poročilih vodi policija ter podatke, ki smo jih uspeli pridobiti s pomočjo spleta.

Tudi na podlagi policijskih poročil ne pridemo do celovitih dejanskih podatkov o zlorabah plačilnih kartic. Razlog lahko poiščemo v neuspešnosti policije pri zbiranju dokazov ali pa v pomanjkanju prijav storitve kaznivega dejanja s strani oškodovancev. Policija v svojih poročilih tako beleži le evidenco o obravnavanih zlorabah, za katere so podane kazenske ovadbe. Zavedati se moramo, da je zlorab veliko več, kot se jih vodi v policijskih evidencah.

Tabela 6: Število kaznivih dejanj gospodarske kriminalitete ter povzročena škoda

Kaznivo dejanje gospodarske kriminalitete	**Število kaznivih dejanj**				**Škoda v tisoč EUR**				**Člen KZ**
	2009	**2010**	**2011**	**½ 2012**	**2009**	**2010**	**2011**	**½ 2012**	
Uporaba ponarejenega negotovinskega plačilnega sredstva	424	1.075	710	146	190,8	209	254,1	127,6	247.
Zloraba negotovinskega plačilnega sredstva	774	428	401	15	64,4	136,4	54,1	10,4	253.

Vir: Policija, Poročilo o delu policije za leto 2010, 2010, str. 36.; Policija, Poročilo o delu policije za leto 2011, 2011, str. 63.; Policija, Poročilo o delu policije za prvo polletje 2012, 2012, str. 12.

Iz tabele št. 6, ki prikazuje število kaznivih dejanj gospodarske kriminalitete ter s tem povzročeno škodo v tisoč € po členih 247. in 253. KZ, je moč razbrati, da je v letu 2011 v primerjavi z letom 2010 manj obravnavanih obeh kazenskih dejanj, in sicer tako uporabe ponarejenega negotovinskega plačilnega sredstva (247. člen KZ), kot tudi zlorab negotovinskega plačilnega sredstva (253. člen KZ). Kljub manjšemu številu uporabe ponarejenih negotovinskih sredstev, je škoda v letu 2011 višja kot v letu 2010. Podatki za prvo polletje leta 2012 kažejo na zmanjšanje števila kaznivih dejanj, žal pa na mnogo višjo povzročeno škodo. Glede zlorabe negotovinskega plačilnega sredstva (izdaje nekritega čeka in zlorabe bančne ali kreditne kartice) opazimo trend zmanjševanja tako kaznivih dejanj kot tudi povzročene škode, kar je vsekakor dobrodošlo in pozitivno.

Tabela 7: Število kaznivih dejanj in ovadenih osumljencev računalniške kriminalitete

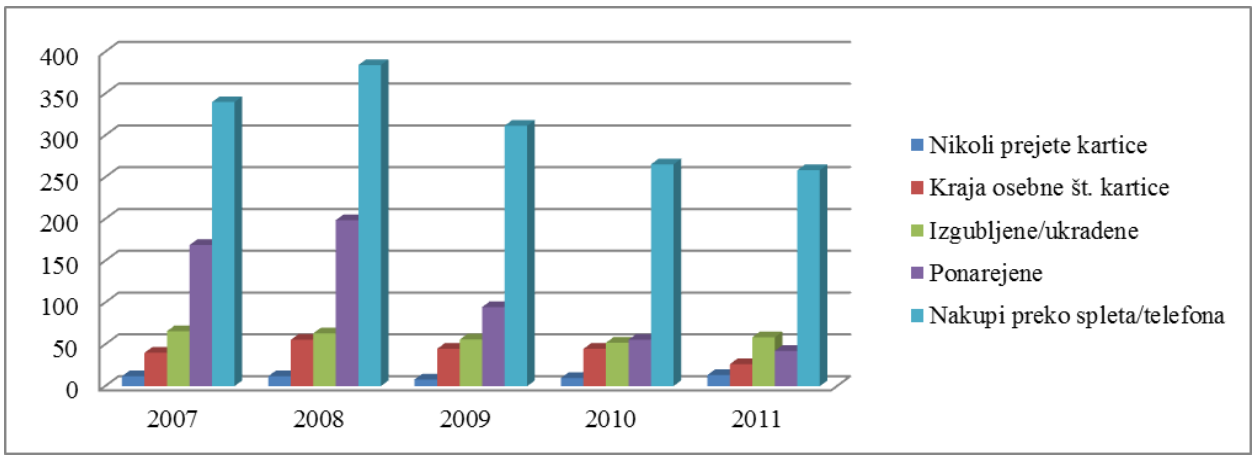
Kaznivo dejanje računalniške kriminalitete	**Število kaznivih dejanj**				**Št. ovadenih osumljencev**				**Člen KZ**
	2009	**2010**	**2011**	**½ 2012**	**2009**	**2010**	**2011**	**½ 2012**	
Napad na informacijski sistem	98	76	236	64	78	25	184	15	221.
Vdor v računalniški sistem	11*	15*	25	5	6	1	21	2	242.

Legenda: * skupaj z zlorabami osebnih podatkov.

Vir: Policija, Poročilo o delu policije za leto 2010, 2010, str. 38.; Policija, Poročilo o delu policije za leto 2011, 2011, str. 64.; Policija, Poročilo o delu policije za prvo polletje 2012, 2012, str. 13.

Tabela št. 7 prikazuje število kaznivih dejanj in ovadenih osumljencev računalniške kriminalitete po členih 221. in 242. KZ. Opaziti je visok porast števila obeh kaznivih dejanj, to je napad na informacijski sistem (221. člen KZ) in vdor v računalniški sistem (242. člen KZ). Tudi število ovadenih oseb se je v letu 2011 v primerjavi z letom 2010 zelo povečalo.

*Slika 1: Izgube kartic glede na vrsto zlorabe v Združenem kraljestvu**



Legenda: * Preračunano iz funtov v eure po osrednjem tečaju BS na dan 18. 4. 2013.

Vir: Card Fraud, 2013.

Slika št. 1 prikazuje izgube kartic glede na vrsto zlorabe v mio € v Združenem kraljestvu. Vidimo, da se daleč največ izgub kartic zgodi z nakupi prek spleta ali telefona (angl. *card not present – CNP fraud*). Sledijo zlorabe s ponarejenimi karticami (angl. *counterfeit fraud*), ki pa so v letu 2011 dosegle nižje izgube v primerjavi z izgubljenimi ali ukradenimi karticami (angl. *stolen/lost fraud*), za katere bi lahko rekli, da skozi leta povzročajo konstantno izgubo. Poglavitni razlog za zmanjšanje izgube s ponarejenimi karticami gre vsekakor iskati v uvedbi EMV standarda. Glede na obseg izgube sledi kraja osebne številke kartice (angl. *card ID theft*), ki se je v letu 2011 nekoliko znižala v primerjavi s prejšnjimi leti. Na zadnjem mestu, sicer s konstantno izgubo, pa je zloraba nikoli prejete kartice (angl. *mail non-receipt fraud*).

Tabela 8: Prehod na EMV standard v EU

	2007 v %	**2008 v %**	**2009 v %**	**2010 v %**
Bankomati	81	91	92	96
POS terminali	65	74	80	90
Kartice	60	67	71	81

Vir: European Central Bank, Report on card fraud, 2012, str. 11.

V tabeli št. 8 so za EU območju prikazani odstotki prehodov bankomatov, POS terminalov in kartic na EMV standard. Podatki so z vidika zlorab plačilnih kartic zelo spodbudni (kar je jasno razvidno na sliki št. 1, saj je v letu 2011 najmanjša izguba zaradi zlorab kartic v primerjavi z ostalimi leti). Glavni problem z vidika varnosti plačilnih kartic še vedno predstavljajo magnetni zapisi na karticah, ki so še vedno prisotne zaradi držav, ki še niso sprejele EMV standarda. Ne smemo pa pozabiti na dejstvo, da kljub karticam brez magnetnega zapisa v prihodnosti, zlorabe ne bodo izginile. Samo vprašanje časa je, kdaj bodo storilci odkrili nove naprave, s katerimi bo mogoče »prebrati« tudi zapis na čipu kartice.

3 ANALIZA PONUDB PLAČILNIH KARTIC PRI SLOVENSKIH BANKAH

V poglavju 3.1 bomo tabelarično prikazali ponudbo plačilnih kartic pri slovenskih bankah, hranilnicah in podružnici. Nato bomo v poglavju 3.2 predstavili analizo stroškov blokacije, nadomestila za opcijo SMS (angl. *Short Message Service*) ter zavarovanje plačilnih kartic. V poglavju 3.3 pa se bomo podrobneje posvetili analizi stroškov dviga z debetno in kreditno plačilno kartico ter letnega nadomestila za kreditno plačilno kartico.

3.1 PONUDBA PLAČILNIH KARTIC PRI SLOVENSKIH BANKAH, HRANILNICAH IN PODRUŽNICI

S pregledom ponudbe plačilnih kartic pri slovenskih bankah, hranilnicah in podružnici smo želeli prikazati vrste plačilnih kartic, ki so dostopne na slovenskem trgu. Iz tabele št. 9 je razvidno, da je med vsemi slovenskimi bankami, hranilnicami in podružnico kar 14 takih, ki imajo v svoji ponudbi plačilno kartico Activa Maestro, takoj za tem sledi ponudba Active MasterCard ter zlate

Active MasterCard. Plačilni kartici BA Maestro ter MasterCard ima v svoji ponudbi 8 bank ter ena hranilnica, zlato MasterCard plačilno kartico pa ponuja ena banka manj. V ponudbi na slovenskem bančnem trgu najdemo še Viso, Activo Viso, predplačniško kartico ter Karanto. Plačilno kartico American Express pa ima v svoji ponudbi samo Banka Koper d.d.

Tabela 9: Pregled ponudbe plačilnih kartic pri slovenskih bankah, hranilnicah in podružnici

Naziv ponudnika plačilnih storitev	BA Maestro	Master Card	Zlata Master Card	Visa	Activa Visa	Activa Maestro	Activa Master Card	Zlata Activa Master Card	Predplačni-ška kartica	American Express	Karanta
Abanka d.d.	x	x		x					x		
Banka Celje d.d.					x	x	x	x			
Banka Koper d.d.					x	x	x	x	x	x	
Sparkasse d.d.	x	x	x								
BKS Bank AG						x	x	x			
Delavska hran. d.d.	x	x	x								
DBS d.d.						x	x	x			
Factor banka d.d.	x	x									
Gorenjska banka d.d.						x	x	x			
Hran. Vipava d.d.						x					
Hran. Lon d.d.						x	x				
Hypo d.d.	x	x	x								
NLB d.d.	x	x	x	x							x
NKBM d.d.					x	x	x	x			x
PBS d.d.					x	x	x	x			
Probanka d.d.						x	x	x			
Raiffeisen d.d.						x	x	x			
Sberbank d.d.						x	x	x			
SKB d.d.	x	x	x	x		x					
Unicredit d.d.	x	x	x			x	x	x			

Vir: Kartice, 2013a; Kartice, 2013b; Plačilne kartice, 2013a; Paketni račun kartice, 2013; Plačilne kartice, 2013b; Navadna kartica, 2013; Plačilne kartice, 2013c; Kartice, 2013c; Plačilne kartice, 2013d; Hranilnica Vipava d.d., 2013; Plačilne in kreditne kartice, 2013; Kartice, 2013d; Plačilne kartice, 2013e; Kartice in Moneta, 2013; Plačilne kartice, 2013f; Plačilne kartice, 2013g; Kartice 2013e; Activa Maestro, 2013; Kartice, 2013f; Kartice 2013g.

3.2 ANALIZA STROŠKOV BLOKACIJE, NADOMESTILA ZA OPCIJO SMS TER ZAVAROVANJE PLAČILNIH KARTIC

Analizo stroškov »blokacije« debetne in kreditne plačilne kartice, ki omogoča preklic veljavnosti kartice, ponudbe varnostnih sporočil SMS, stroškov nadomestila za opcijo varnostni SMS ter analize možnosti zavarovanja plačilnih kartic pred zlorabo, skupaj z navedbo zavarovalnice, pri kateri posamezna banka, hranilnica ali podružnica ponuja to možnost, ter zneske plačila letne premije za zavarovanje smo prikazali v tabeli št. 10. Strošek blokacije zaradi kraje ali suma zlorabe bo imetnika debetne plačilne kartice v povprečju stal 7,61 €, kreditne plačilne kartice pa 10,67 €. Ob tem ne smemo pozabiti na dejstvo, da je potrebno ob blokaciji plačilne kartice

naročiti novo, kar pomeni dodatni strošek za imetnika. Opcijo »varnostni SMS« ponuja kar 17 od 20 ponudnikov plačilnih storitev, saj se vedno bolj zavedajo pomena preventivnih ukrepov glede zlorabe plačilnih kartic. Povprečen mesečni strošek za opcijo »varnostni SMS« znaša 0,75 €. Zavarovanje plačilnih kartic pred zlorabo ponuja le 10 ponudnikov plačilnih storitev. Glede na to, da znaša povprečna letna premija 8,20 €, verjamemo, da se bo v prihodnje število ponudnikov kot tudi povpraševalcev po takšnem zavarovanju še povečalo.

Tabela 10: Analiza stroškov blokacije, nadomestila za opcijo SMS ter zavarovanja plačilnih kartic

Naziv ponudnika plačilnih storitev	**Blokacija zaradi kraje ali suma zlorabe - debetna kartica v EUR**	**Blokacija zaradi kraje ali suma zlorabe - kreditna kartica v EUR**	**Varnostni SMS**	**Strošek nadomestila za opcijo varnostni SMS v EUR**	**Zavarovanje plačilnih kartic pred zlorabo**	**Zavarovanje plačilnih kartic pri zavarovalnici**	**Letna premija za zavarovanje kartic v EUR**
Abanka d.d.	5,20	8,40	DA	1,00	DA	Triglav	9,90
Banka Celje d.d.	12,52	20,87	DA[1]	/	NE	/	/
Banka Koper d.d.	6,90	9,00	DA	0,50	NE	/	/
Sparkasse d.d.	6,00	20,86	DA[2]	0,00	DA	Triglav	8,50
BKS Bank AG	6,30	6,30	DA	0,70	NE	/	/
Delavska hranilnica d.d.	6,20	12,50	DA	0,50	NE	/	/
DBS d.d.	6,50	8,50	DA	1,00	DA	Tilia	Np
Factor banka d.d.	6,00	6,30	NE	/	NE	/	/
Gorenjska banka d.d.	5,30	6,40	DA	1,10	DA	Triglav	9,00
Hranilnica Vipava d.d.	6,00	/	NE	/	NE	/	/
Hranilnica Lon d.d.	8,95	12,00	DA	0,65	NE	/	/
Hypo d.d.	6,75	6,75	DA	1,02	DA	Triglav	9,00
NLB d.d.	6,70	6,70	DA	1,00	DA	Triglav	9,00
NKBM d.d.	6,68	8,93	DA	0,70	DA	Maribor	7,20
PBS d.d.	9,00	9,00	DA	0,70	NE	/	/
Probanka d.d.	7,20	8,60	DA	1,00	DA	Maribor	8,00
Raiffeisen d.d.	3,00	9,99	DA	0,00	DA	Uniqa	5,00
Sberbank d.d.	10,00	15,00	DA	1,00	NE	/	/
SKB d.d.	7,00	6,60	NE	/	DA	Triglav	4,54[3] /7,00[4]
Unicredit d.d.	20,00	20,00	DA	1,20	NE	/	/

Legenda: [1]samo za uporabo elektronske banke; [2]za paketne račune; [3]za MasterCard kartico; [4]za Visa kartico; np - ni podatka.

Vir: Cene in obrestne mere, 2013; Ceniki, 2013a; Tarifa banke, 2013; Obrestne mere, 2013; Vezane vloge depoziti, 2013; Tarife – Občani, 2013; Tarife in obrestne mere, 2013; Cenik poslovanja, 2013; Tarife nadomestila, 2013; Tarife plačil, 2013; Tarife, 2013a; Ceniki, 2013b; Stroški in obrestne mere, 2013; Ceniki storitev, 2013a; Cenik osebne finance, 2013; Tarife, 2013b; Tarife, 2013c; Cenik storitev, 2013b; Ceniki, 2013c; Izvleček iz tarife poslovanja s prebivalstvom, 2013.

3.3 ANALIZA STROŠKOV DVIGA Z DEBETNO IN KREDITNO PLAČILNO KARTICO TER LETNEGA NADOMESTILA ZA KREDITNO PLAČILNO KARTICO

Imetnike plačilnih kartic zanimajo predvsem stroški, povezani s karticami. Zato smo v tabeli št. 11 prikazali stroške dviga gotovine na bančnem avtomatu ali okencu pri posameznih ponudnikih plačilnih storitev, opravljenega z debetno plačilno kartico. V tabeli niso navedeni stroški za dvig gotovine na lastnem bančnem avtomatu ponudnikov, saj dviga na lastnem bančnem avtomatu ne zaračunava nobeden od spodaj navedenih ponudnikov plačilnih storitev. Povprečen strošek za dvig gotovine na bančnem avtomatu druge banke (v državi in čezmejno v EUR območju) znaša 0,23 €, za dvig opravljen v tretji državi (izven EUR območja) pa kar 2,25 €. Najugodnejši sta Banka Sparkasse d.d. in Delavska hranilnica d.d., najdražja pa je Banka Celje d.d. Minimalni povprečni strošek za dvig gotovine na bančnem okencu druge banke (v državi in čezmejno v EUR območju) znaša 1,92 €, za dvig opravljen v tretji državi (izven EUR območja) pa 2,12 €. Tudi pri dvigu na bančnem okencu sta z 1,67 € najugodnejši Banka Sparkasse d.d. in Delavska hranilnica d.d., najdražja pa je tokrat z 2,75 € Nova KBM d.d.

Tabela 11: Analiza stroškov dviga gotovine na bančnem avtomatu in okencu z debetno plačilno kartico

Naziv ponudnika plačilnih storitev	**Bankomat druge banke - v državi in čezmejno v EUR**	**Bankomat drugega ponudnika plačilnih storitev - v tretji državi v % (v EUR)**	**Okence pri drugi banki - v državi in čezmejno v % (v EUR)**	**Okence pri drugi banki - v tretji državi v % (v EUR)**
Abanka d.d.	0,50	1,00 (min 2,10, max 22,00)	1,00 (min 2,10, max 22,00)	1,00 (min 2,10, max 22,00)
Banka Celje d.d.	0,50	(2,85)	(1,60)	(2,85)
Banka Koper d.d.	0,53	(2,65)	(2,65)	(2,65)
Sparkasse d.d.	0,00	1,00 (min 1,67, max 12,52)	1,00 (min 1,67, max 12,52)	1,00 (min 1,67, max 12,52)
BKS Bank AG	0,00	1,00 (min 1,70)	-	-
Delavska hranilnica d.d.	0,00	1,00 (min 1,67, max 20,00)	1,00 (min 1,67, max 20,00)	1,00 (min 1,67, max 20,00)
DBS d.d.	0,00	(1,80)	2,00%	-
Factor banka d.d.	0,00	1,00 (min 1,70, max 20,85)	1,00 (min 1,70, max 20,85)	1,00 (min 1,70, max 20,85)
Gorenjska banka d.d.	0 (0,45 v bližini GB bankomatov)	1,00 (min 2,73)	2,00 (dvig možen samo na PBS)	1,00 (min 2,73)
Hranilnica Vipava d.d.	0,00	(2,50)	(2,50)	(2,50)
Hranilnica Lon d.d.	0,00	1,50 (min.2,25, max.6,71)	-	-
Hypo d.d.	0,45	1,00 (min 1,80, max 22,25)	1 (min 1,80, max 22,25)	1,00 (min 1,80, max 22,25)
NLB d.d.	0,51	1,00 (min 2,14 in max 22,46)	1 (min.2,14 in max.22,46)	1,00 (min 2,14 in max.22,46)
NKBM d.d.	0,48	(2,75)	(2,75)	(2,75)
PBS d.d.	0,45	(2,80)	2,00	2,00
Probanka d.d.	0,43 (od 6. dviga v mesecu dalje)	1,30 (min 2,70)	1,30 (min 2,70)	1,30 (min 2,70)
Raiffeisen d.d.	0,00	(2,50)	(2,50)	-

se nadaljuje

nadaljevanje

Naziv ponudnika plačilnih storitev	Bankomat druge banke - v državi in čezmejno v EUR	Bankomat drugega ponudnika plačilnih storitev - v tretji državi v % (v EUR)	Okence pri drugi banki - v državi in čezmejno v % (v EUR)	Okence pri drugi banki - v tretji državi v % (v EUR)
Sberbank d.d.	0,00	(2,50)	(2,50)	(2,50)
SKB d.d.	0,45	1,10 (min 2,20, max 22,50)	1,10 (min 2,20, max 22,50)	1,10 (min 2,20, max 22,50)
Unicredit d.d.	0,33 (od 4. dviga dalje)	1,00 (min.2,00, max 21,00)	1,00 (min 2,00, max 21,00)	1,00 (min 2,00, max 21,00)

Vir: Cene in obrestne mere, 2013; Ceniki, 2013a; Tarifa banke, 2013; Obrestne mere, 2013; Vezane vloge depoziti, 2013; Tarife – Občani, 2013; Tarife in obrestne mere, 2013; Cenik poslovanja, 2013; Tarife nadomestila, 2013; Tarife plačil, 2013; Tarife, 2013a; Ceniki, 2013b; Stroški in obrestne mere, 2013; Ceniki storitev, 2013a; Cenik osebne finance, 2013; Tarife, 2013b; Tarife, 2013c; Cenik storitev, 2013b; Ceniki, 2013c; Izvleček iz tarife poslovanja s prebivalstvom, 2013.

Ker ima veliko uporabnikov debetne plačilne kartice v svojih denarnicah tudi kreditno plačilno kartico, smo v tabeli št. 12 prikazali strošek dviga gotovine ter letno nadomestilo za klasično in zlato kreditno kartico. Minimalni povprečni strošek za dvig gotovine v državi in čezmejno v EUR območju, kot tudi v tretjih državah, znaša 8,21 €. Tudi pri dvigu s kreditno kartico je z minimalnim stroškom 4,17 € najugodnejša Banka Sparkasse d.d., najdražja pa je NLB d.d. z 12,80 €. Povprečen strošek letnega nadomestila za uporabo klasične kreditne kartice znaša 18,02 € ter za zlato kreditno kartico 50,66 €. Letno nadomestilo za klasično kreditno kartico je z 12,50 € najcenejše pri Delavski hranilnici d.d. ter s 25,00 € najdražje na Unicredit banki d.d. Najcenejše letno nadomestilo za zlato kreditno kartico, to je 24,90 €, zaračunajo na Raiffeisen banki d.d., najdražje pa na NLB d.d., kjer znaša 71,41 €.

Tabela 12: Analiza stroškov dviga gotovine ter letnega nadomestila za klasično in zlato kreditno kartico

Naziv ponudnika plačilnih storitev	Dvig gotovine v državi in čezmejno v % (v EUR)	Dvig gotovine v tretji državi v % (v EUR)	Letno nadomestilo za klasično kreditno kartico[1] v EUR	Letno nadomestilo za zlato kreditno kartico[1] v EUR
Abanka d.d.	5,00 (min 12, max 125,50)	5,00 (min 12, max 125,50)	17,00	/
Banka Celje d.d.	5,00 (min 8)	5,00 (min 8)	15,63	53,59
Banka Koper d.d.	5,00 (min 6,25)	5,00 (min 6,25)	17,65	64,20
Sparkasse d.d.	5,00 (min 4,17, max 20,86)	5,00 (min 4,17, max 20,86)	17,00	34,00
BKS Bank AG	4,50 (min 7)	4,50 (min 7)	22,00	40,00
Delavska hran. d.d.	3,50 (min 8, max 20)	3,50 (min 8, max 20)	12,50	32,50
DBS d.d.	5,00 (min 5,90)	5,00 (min 5,90)	16,30	58,70
Factor banka d.d.	4,00 (min 8, max 125,20)	4,00 (min 8, max 125,20)	15,50	/
Gorenjska banka d.d.	5,00 (min 7,70)	5,00 (min 7,70)	18,00	68,00
Hran. Vipava d.d.	/	/	/	/
Hranilnica Lon d.d.	5,00 (min 10,5, max 20)	5,00 (min 10,5, max 20)	14,50	/
Hypo d.d.	5,00 (min 8,90, max 133)	5,00 (min 8,90, max 133)	20,30	53,50
NLB d.d.	3,70 (min 12,80)	3,70 (min 12,80)	19,26	71,41
NKBM d.d.	5,00 (min 6,50)	5,00 (min 6,50)	16,00	60,00

se nadaljuje

nadaljevanje

Naziv ponudnika plačilnih storitev	Dvig gotovine v državi in čezmejno v % (v EUR)	Dvig gotovine v tretji državi v % (v EUR)	Letno nadomestilo za klasično kreditno kartico[1] v EUR	Letno nadomestilo za zlato kreditno kartico[1] v EUR
PBS d.d.	5,00 (min 7)	5,00 (min 7)	17,50	55,00
Probanka d.d.	4,50 (min 9,10)	4,50 (min 9,10)	16,20	32,00
Raiffeisen d.d.	5,00 (min 7)	5,00 (min 7)	19,90	24,90
Sberbank d.d.	5,00 (min 6,5)	5,00 (min 6,5)	20,00	60,00
SKB d.d.	5,40 (min 8,7)	5,40 (min 8,7)	22,08	52,80
Unicredit d.d.	5,00 (min 12)	5,00 (min 12)	25,00	50,00

Legenda: [1]za osnovni račun.

Vir: Cene in obrestne mere, 2013; Ceniki, 2013a; Tarifa banke, 2013; Obrestne mere, 2013; Vezane vloge depoziti, 2013; Tarife – Občani, 2013; Tarife in obrestne mere, 2013; Cenik poslovanja, 2013; Tarife nadomestila, 2013; Tarife plačil, 2013; Tarife, 2013a; Ceniki, 2013b; Stroški in obrestne mere, 2013; Ceniki storitev, 2013a; Cenik osebne finance, 2013; Tarife, 2013b; Tarife, 2013c; Cenik storitev, 2013b; Ceniki, 2013c; Izvleček iz tarife poslovanja s prebivalstvom, 2013.

4 RAVNANJE BANKE X V PRIMERU SUMA ZLORABE PLAČILNIH KARTIC

Banke se morajo kot izdajateljice plačilnih kartic zavedati tveganja oziroma dejstva, da lahko pride do zlorab. To ne pomeni, da bodo zlorabljene vse izdane plačilne kartice, določen odstotek pa bo skoraj zagotovo. Ravno zato je za banke izdajateljice zelo pomembno, da se zavedajo, da je postopek preprečevanja zlorab na prodajnih mestih (opremljenih s POS terminali) in bančnih avtomatih, kjer se kot plačilno sredstvo sprejemajo kartice, zelo pomemben. Seveda se morajo banke v prvi vrsti držati zakonskih predpisov, upoštevati zahteve oziroma priporočila (s strani ZBS, Policije, Banke Slovenije, Slovenskega zavarovalnega združenja in ostalih), predpisane varnostne standarde (glede plačilnih kartic, bančnih avtomatov, POS terminalov in ostalega), kot tudi sprejeti vse aktivnosti za obvladovanje tveganj, s katerimi se srečujejo.

Banke morajo, če želijo kar se da zmanjšati možnosti zlorab, v vseh pogledih delovati preventivno ter korektivno, v primeru zlorabe oziroma incidenta pa seveda tudi ustrezno ukrepati z namenom preprečevanja nadaljnjih zlorab. To med drugim pomeni tudi, da mora banka kot izdajatelj plačilnih kartic oziroma kot strokovnjak na področju izdajanja plačilnih kartic imetnikom omogočiti ustrezne postopke za obveščanje o kraji ali izgubi plačilne kartice ter zagotoviti takojšen preklic plačilne kartice v elektronskem komunikacijskem sistemu (Trstenjak, 2003, str 24-25).

Mejač Krassnig (2012, str. 1) pravi, da je za banko pomembno, da s svojimi aktivnostmi obvladuje tveganja, ki se jim izpostavlja:

- kot lastnica infrastrukture (POS terminali in bančni avtomati),
- v odnosu do imetnikov,
- v odnosu do prodajnih mest,

- v odnosu do dobaviteljev (programske opreme),
- v odnosu do izvajalcev in
- skrbi za stalno strokovno izpopolnjevanje zaposlenih ter
- preprečuje zlorabe in incidentno ukrepa.

Dejstvo, da so zlorabe nepredvidljive in da so kriminalci skoraj vedno vsaj en korak pred mehanizmi varnosti, pripelje do spoznanja, da je najpomembnejše preventivno ukrepanje, tako s strani izdajateljev, kot tudi imetnikov plačilnih kartic. Preventiva in ozaveščenost zagotovo pripomoreta k zmanjšanju števila zlorab plačilnih kartic.

Glede na tematiko diplomskega dela je smiselno, da se seznanimo tudi s tveganji pri poslovanju z bančnimi avtomati (Bertoncelj, 2012, str. 10-14):

- operativna tveganja,
- tveganje izgube dobrega imena,
- tveganje človeških virov,
- tveganje opravljanja poslovnih procesov,
- tveganje informacijskega premoženja,
- tehnična tveganja in
- tveganja kaznivih dejanj.

V nadaljevanju si bomo pogledali postopek ravnanja banke X (zaradi občutljivosti podatkov bo banka ostala anonimna) v primeru suma zlorabe plačilnih kartic (skimminga) in delovna navodila za ravnanje bančnih delavcev v primeru zlorabe na bančnih avtomatih. Na koncu poglavja pa se bomo seznanili s statističnimi podatki o zlorabah na banki X.

4.1 PROCES RAVNANJA BANKE X V PRIMERU SUMA ZLORABE PLAČILNIH KARTIC

V procesu banke X v primeru suma zlorabe plačilnih kartic sodeluje, oziroma deluje več oddelkov, in sicer:

- oddelek Pasivnih poslov (v nadaljevanju OPP), ki spada pod sektor Financ,
- oddelek Zaledje, ki spada pod sektor Financ,
- pooblaščena oseba odgovorna za varnost na banki X,
- pooblaščene kontaktne osebe banke X,
- poslovni tehnolog za področje kartičnega poslovanja in
- zaposleni v Centru bančnih storitev in informacij (v nadaljevanju CBSI).

Banka se ob izdaji plačilnih kartic srečuje tudi z zlorabo plačilnih kartic. O zlorabi govorimo takrat, ko je uporaba plačilne kartice opravljena s strani nepooblaščene tretje osebe. Najpogostejša načina zlorabe sta spletne prevare in kopiranje magnetnega zapisa s plačilne kartice brez vednosti in soglasja imetnika kartice. Takšni obliki zlorabe se praviloma zgodita na

mestih, kjer mora uporabnik kartice prek številčnice vtipkati tudi PIN številko. Seveda obstajajo tudi drugačni načini zlorab kartic, ki pa niso tako množični.

Lastnik licence MasterCard in izdajatelji kartic se trudijo, da bi tako nastalo škodo čim bolj omilili, saj se je v celoti ne da preprečiti. Ena od zaščit izdajatelja kartic je obveščanje o nepooblaščenih posegih v najkrajšem možnem času, zato je potrebno že ob podani zahtevi za pridobitev licence za izdajo kartičnih produktov MasterCardu sporočiti ime osebe, ki je odgovorna za varnost na strani izdajatelja plačilnih kartic.

Prav tako ima banka na podlagi priporočila ZBS določene pooblaščene kontaktne osebe, ki so določene s sklepom uprave. Le-te morajo biti dosegljive 24 ur na dan, 7 dni v tednu, in se v imenu banke v najkrajšem možnem času odločajo in sprejemajo ustrezne varnostne ukrepe, če presodijo, da je to potrebno. Njihova naloga je tudi obveščanje ostalih ustreznih služb oziroma oddelkov v banki. Ravno tako mora imeti kontaktna oseba zadosti strokovnega znanja o kartičnem poslovanju, da lahko v najkrajšem možnem času sprejme primerno poslovno odločitev v dobro banke in na ta način zmanjša škodo, ki lahko nastane zaradi zlorabe plačilnih kartic. Seveda je razumljivo tudi dejstvo, da popolna preprečitev škode iz tega naslova ni možna.

Slovenske banke so se za zaščito svojih komitentov organizirale tako, da so v proces medsebojnega obveščanja vključile svoje procesne centre. Procesni centri so namreč tisti, ki prvi zaznajo povečan prejem reklamacijskih zahtevkov. Takoj, ko kateri koli slovenski procesni center zazna nek skupen vzrok reklamacij (primer: skimming na nekem bankomatu), ukrepa na naslednji način:

- pripravi seznam kartic, ki so bile uporabljene na kritičnem mestu,
- po telefonu in/ali po elektronski pošti obvesti pooblaščene kontaktne osebe banke o sumljivem dogajanju,
- pooblaščenim kontaktnim osebam pošlje naziv prodajnega mesta (POS terminala ali bančnega avtomata) in okvirni čas, ko naj bi do zlorab prihajalo.

Sum zlorabe plačilne kartice ali odkrita snemalna naprava na nekem prodajnem mestu še ne pomeni, da bo do zlorabe dejansko prišlo. Previdnost v takšnih primerih ni nikoli odveč. Za čim boljše ukrepanje (da se lahko čim bolj natančno identificira vse tiste plačilne kartice, ki so bile nevarnosti izpostavljene) je zelo pomembna natančna določitev časovnega obdobja, kdaj je bila snemalna naprava nameščena na nekem prodajnem mestu. Slednje zagotovo ni enostavno, saj vemo, da takšne naprave po navadi odkrijejo šele po preteku kar nekaj časa. Če imamo v mislih bančni avtomat, ki je postavljen nekje v središču velikega mesta, kjer je frekvenca dvigov zelo visoka, lahko samo slepo ugibamo, za kako velik nabor različnih plačilnih kartic s potencialno možnostjo zlorabe v prihodnosti gre.

4.1.1 Prejem obvestila o sumu zlorabe plačilnih kartic

Pooblaščene kontaktne osebe banke X lahko prejmejo obvestilo o sumljivih transakcijah s strani:

- Bankarta,

- pooblaščene kontaktne osebe katere koli druge banke,
- sektorja Financ, oddelka Zaledje (obvestilo prek aplikacije MasterCard Online).

Obvestilo se pridobi ali po telefonu ali po elektronski pošti, oziroma v večini primerov kar po obeh poteh. Pooblaščene kontaktne osebe banke X prejmejo obvestilo o dvomljivih transakcijah, ki so lahko med drugim posledica nameščene snemalne naprave na bankomatu.

Prejeto obvestilo lahko vsebuje naslednje informacije:
- nameščena snemalna naprava na bankomatu banke X,
- nameščena snemalna naprava na bankomatu druge banke.

Dolžnost pooblaščenih kontaktnih oseb je, da takoj po prejetju obvestila postopajo v skladu s priporočili ZBS ter internimi delovnimi navodili banke X.

Prejem obvestila o sumu zlorabe pooblaščene kontaktne osebe drugih bank ali Bankarta

V primeru, ko pooblaščene osebe banke X prejmejo obvestilo o sumu zlorabe s strani pooblaščene osebe druge banke ali Bankarta po telefonu in/ali po elektronski pošti, morajo ukrepati skladno s prejeto informacijo, kar pomeni, da lahko:
- podajo zahtevo za blokacijo kartic, ki so bile uporabljene na spornem prodajnem mestu oziroma bankomatu, direktno na Bankart,
- informacijo z dodatnimi navodili posredujejo v OPP,
- sprejmejo obvestilo le na znanje.

Ko pooblaščene osebe banke X prejmejo obvestilo o sumu zlorabe in to obvestilo vsebuje tudi informacijo, da je že prišlo do zaznanih transakcij oziroma avtorizacij po plačilnih karticah, morajo nemudoma podati zahtevo za blokacijo kartic. Pooblaščene kontaktne osebe so pristojne tudi za direktno podajo zahteve Bankartu za blokacijo kartic. Zahteva za blokacije se lahko poda ali po elektronski pošti ali po telefonu. V kolikor do samih transakcij na plačilnih karticah še ni prišlo, ampak obstaja le sum zlorabe, morajo pooblaščene kontaktne osebe banke X po elektronski pošti posredovati informacijo z nadaljnjimi navodili v OPP, pri tem pa morajo upoštevati tudi delovno navodilo banke X, opisano v poglavju 4.1.1 (podpoglavje z naslovom: Posredovanje obvestila o sumu zlorabe plačilnih kartic v oddelek Pasivnih poslov).

Prejem obvestila o sumu zlorabe s strani sektorja Financ

V sektorju Financ oziroma bolj natančno v oddelku Zaledje ima zaposleni dostop do MasterCard Online spletne aplikacije, ki avtomatično kreira elektronska sporočila o karticah, ki so bile uporabljene na sumljivih prodajnih mestih in zanje posledično obstaja možnost zlorabe. Seveda mora zaposleni oddelka Zaledje v primeru prejetja takšnega obvestila o tem nemudoma obvestiti oziroma seznaniti pooblaščene kontaktne osebe banke X, in sicer:
- takoj po prejemu, ali

- prvi delovni dan po prejemu obvestila.

Na podlagi prejetega obvestila, to je ali po elektronski pošti ali po telefonu, morajo pooblaščene kontaktne osebe banke X postopati v skladu s priporočili ZBS in z internimi delovnimi navodili.

Prejem obvestila o nameščeni snemalni napravi na bankomatu, ki je v lasti banke X

Banka X, lastnica bankomata, lahko prejme obvestilo o nameščeni snemalni napravi na bankomatu s strani Bankarta, uporabnika bankomata, uslužbenca banke ali skrbnika bankomata. V takšnem primeru je potrebno informacijo nemudoma posredovati osebi:

- ki je v banki zadolžena za varnost in
- pooblaščenim kontaktnim osebam banke X.

Oseba zadolžena za varnost in pooblaščene kontaktne osebe morajo v takem primeru upoštevati priporočila ZBS ter interna delovna navodila banke za ravnanje bančnih uslužbencev v primeru suma zlorabe na bančnih avtomatih. Ravno tako morajo po elektronski pošti posredovati informacijo z dodatnimi navodili v OPP. Ob prejetju obvestila morajo seveda o tem obvestiti tudi:

- policijo na telefonsko številko 113 oziroma pristojno policijsko postajo (odvisno od lokacije bankomata) in
- 24-urno dežurno službo Bankarta, da izvede obveščanje pooblaščenih oseb drugih bank.

Bančni uslužbenec, ki je lahko tudi pooblaščena kontaktna oseba banke, mora ob prejemu obvestila oziroma ugotovitvi, da je na bankomatu nameščena snemalna naprava:

- zahtevati od 24-urne službe Bankarta, da takoj prekine komunikacijo z bančnim avtomatom,
- poskrbeti, da se bankomat zavaruje, tako da se onemogoči njegovo uporabo vse do prihoda policije, oziroma upošteva navodila policije,
- podati navodilo o zavarovanju bankomata pristojnemu svetovalcu,
- poskrbeti, da se zavarujejo video posnetki,
- iz video posnetkov poskušati ugotoviti termin, ko se je zgodila zloraba in
- ob vzpostavitvi normalnega stanja na bankomatu zahtevati od 24-urne dežurne službe Bankarta ponovno aktiviranje bankomata.

Prejem obvestila o nameščeni snemalni napravi na bankomatu ali POS terminalu, ki ni v lasti banke X

Tudi v primeru, ko banka ni lastnica bankomata ali POS terminala, na katerem je nameščena snemalna naprava, mora biti o tem obveščena. Le na tak način lahko prepreči nadaljnjo škodo kot izdajateljica plačilnih kartic, ki so bile takrat uporabljene na prodajnih mestih z nameščeno snemalno napravo. V tem primeru banka prejme obvestilo o sumu zlorabe plačilnih kartic s strani:

- Bankarta,

- MasterCarda ali
- pooblaščene kontaktne osebe drugih bank.

Obvestilu običajno sledi tudi poročilo o bankomatu ali POS terminalu, kjer naj bi bila nameščena snemalna naprava in časovno obdobje, ko naj bi bila nameščena. V opisanem primeru je potrebno obvestilo nemudoma posredovati pooblaščenim kontaktnim osebam banke in osebi, ki je zadolžena za varnost. Le-te morajo v takšnem primeru upoštevati priporočila ZBS in interna delovna navodila banke ter po elektronski pošti posredovati informacijo z dodatnimi navodili v OPP.

Prejem obvestila o sumu zlorabe velikega števila plačilnih kartic

V primeru, ko pooblaščene kontaktne osebe banke X prejmejo obvestilo o sumu zlorabe velikega števila plačilnih kartic, so potrebni posebni postopki, in sicer se izvede blokacija BIN-a (angl. *Bank Identification Number*, to je začetna številka kartice, ki določa tip kartičnega produkta izdajatelja in je dodeljena s strani imetnika licence), s čimer se administrativno onemogoči uporabo vseh kartic, za katere obstaja sum zlorabe. V takšnih primerih je nujno potrebno sodelovanje z osebo, ki se ukvarja s kartičnim poslovanjem in je pooblaščena za kontaktiranje procesnega centra Bankart, ter soglasje uprave banke. Za tak poseg se seveda odločimo samo takrat, ko ugotovimo, da je prišlo do masovne zlorabe plačilnih kartic, ki je neobvladljiva in je ne moremo preprečiti.

Na samo odločitev o načinu ukrepanja vpliva tudi dejstvo, ali z obvestilom o sumu zlorabe plačilnih kartic prejmemo tudi informacijo:
- da je do zlorabe po karticah že prišlo in/ali
- da je procesni center zaznal avtorizacije po karticah, za katere obstaja velika verjetnost, da so bile uporabljene na nepooblaščen način.

V obeh primerih se kartice blokirajo. V kolikor ne pride do blokacij vseh kartic, za katere obstaja sum zlorabe, se mora postopati na enak način, kot je napisano v poglavju 4.1.1 (podpoglavje z naslovom: Prejem obvestila o sumu zlorabe pooblaščene kontaktne osebe drugih bank ali Bankarta).

Prejem obvestila o sumu zlorabe izven delovnega časa

Banke večinoma poslujejo samo med delovnikom, to je od ponedeljka do petka, v običajnem delovnem času. Zavedati pa se moramo, da so kriminalci na delu večinoma med vikendi, saj je takrat zagotovo večja frekvenca uporabnosti plačilnih kartic, tako na POS terminalih, kot tudi na bankomatih, ter slabši odziv s strani pristojnih služb.

Da bi lahko ukrepali in preprečili nadaljnjo škodo, morajo biti pooblaščene kontaktne osebe bank ter procesni centri vedno dostopni, to pomeni vse dni v letu, ne glede na uro. Zaradi lažje in hitrejše dosegljivosti poteka komunikacija v takšnih primerih večinoma prek mobilnih telefonov.

Zato je v primeru, ko pooblaščena kontaktna oseba banke izven delovnega časa prejme obvestilo po telefonu o sumu zlorabe plačilnih kartic, oziroma o uporabi na rizičnem prodajnem mestu ali bankomatu, na katerem naj bi bila nameščena snemalna naprava, običajna odločitev blokacija vseh kartic. Odločitev, ali se kartice blokirajo ali ne, je odvisna tudi od pridobljene informacije s strani tistega, ki obvešča in sicer:

- od števila izpostavljenih plačilnih kartic,
- kako se na obvestilo odzivajo druge banke in
- ali do zlorabe plačilnih kartic že prihaja.

Posredovanje obvestila o sumu zlorabe plačilnih kartic v oddelek Pasivnih poslov

Obvestilo o sumu zlorabe plačilnih kartic, ki ga prejme pooblaščena kontaktna oseba, se po elektronski pošti posreduje v OPP. Obvestilo vsebuje navodilo za nadaljnje ukrepanje:

- zahteva po obveščanju uporabnikov plačilnih kartic za katere obstaja sum zlorabe ali
- zahteva po obveščanju uporabnikov plačilnih kartic za katere obstaja sum zlorabe in blokacija takih kartic.

V oddelku Pasivni posli postopajo skladno z internim delovnim navodilom, zapisanim v poglavju 4.1.2, ter seveda v skladu z navodili pooblaščene kontaktne osebe bank.

4.1.2 Zlorabe plačilnih kartic in ukrepanje v oddelku Pasivni posli

Pooblaščene kontaktne osebe banke X morajo ob prejemu obvestila o sumu zlorabe plačilnih kartic sprejeti primerno poslovno odločitev v dobro banke ter po elektronski pošti o tem obvestiti sodelavce v OPP. Elektronska pošta vsebuje navodila za nadaljnje ukrepanje, ki je lahko:

- zahteva po obveščanju uporabnikov kartic ali
- zahteva po obveščanju uporabnikov kartic in blokacija takih kartic.

Naloga sodelavcev v OPP, po prejemu obvestila o sumu zlorabe plačilnih kartic oziroma navodil s stani pooblaščene kontaktne osebe, je:

- priprava seznama imetnikov plačilnih kartic, pri katerih obstaja sum zlorabe,
- izvedba obveščanja imetnikov s seznama plačilnih kartic, pri katerih obstaja sum zlorabe in
- dopolnitev seznama imetnikov plačilnih kartic, pri katerih obstaja sum zlorabe s podatki o opravljenih aktivnostih.

Ta naloga se vedno opravlja prioritetno in mora biti rešena v najkrajšem možnem času, kar je odvisno predvsem od količine podatkov, oziroma števila plačilnih kartic, pri katerih obstaja sum zlorabe.

Priprava seznama imetnikov plačilnih kartic, pri katerih obstaja sum zlorabe

Po prejetem obvestilu s strani pooblaščene kontaktne osebe o sumu zlorabe plačilnih kartic je ena izmed naloga OPP tudi priprava ustreznega seznama vseh imetnikov plačilnih kartic, pri katerih obstaja sum zlorabe. Pripravljen seznam je osnova za kontaktiranje imetnikov plačilnih kartic, saj zanje obstaja možnost zlorabe.

Seznam se oblikuje s pomočjo spletne aplikacije »Web Avtorizacijski logi«, ki jo je za banke izdelal procesni center Bankart. Aplikacija omogoča bančnim uslužbencem vpogled v transakcije in podrobnosti o teh transakcijah v realnem času. Razvoj aplikacije je posledica potrebe bank po takojšnjem dostopu do podatkov o transakcijah njihovih komitentov iz različnih naslovov, kot so reševanje reklamacij in pomoč pri analiziranju v primeru zlorab. Glavna prednost aplikacije je, da v svoji podatkovni bazi hrani vse transakcije (prek POS terminalov in bankomatov), avtorizirane na avtorizacijskem sistemu Bankarta. Aplikacija omogoča pregled odobrenih in zavrnjenih transakcij, ne glede na kraj opravljene transakcije (Bankartova mreža POS terminalov in bankomatov, ostale mreže v Sloveniji ali tujini), v realnem času. Zaradi varstva podatkov je dostop do aplikacije pogojen s certifikatom, uporabniškim imenom in geslom. Aplikacija podpira tri različne nivoje dostopa, glede na vrsto uporabnikov:

- prvi nivo: namenjen referentom, omogoča preglede osnovnih podatkov,
- drugi nivo: namenjen tistim, ki se ukvarjajo z reklamacijami, saj imajo možnost vpogleda v vse transakcije (tako izdajatelja kot prejemnika) in
- tretji nivo: namenjen tehnologom in drugim strokovnim delavcem v bankah, saj imajo poleg pravic drugega nivoja še dostop do dokumentacije in poročil.

Prikaz podatkov s pomočjo spletne aplikacije ter dopolnjeni podatki po obdelavi so razvidni iz Priloge 5.

Obveščanje imetnikov plačilnih kartic o možnosti zlorabe njihovih kartic

Na podlagi pripravljenega ustreznega seznama vseh imetnikov plačilnih kartic za katere obstaja sum zlorabe v OPP izvedejo obveščanje, in sicer preko:

- telefona,
- elektronske pošte (vsebina poslanega obvestila je enaka vsebini pisnega obvestila) in
- navadne pošte (kot navadna poštna pošiljka).

Po potrebi se uporabi tudi vse tri naštete načine obveščanje strank, v kolikor se stranke ne uspe priklicati, ali če ni dosegljiva po elektronski pošti. Ob tem se imetnike plačilnih kartic za katere obstaja sum zlorabe seznani z dejstvom, da obstaja možnost, da bo njihova plačilna kartica zlorabljena ter se stranki, glede na vrsto kartice, priporoči nadaljnje ukrepe.

V kolikor je stranka imetnik BA Maestro kartice se ji predlaga ali menjavo osebnega gesla (kar lahko imetniki storijo sami na bankomatu, ki je v lasti banke izdajateljice plačilne kartice) ali blokacijo kartice in naročilo nove, nadomestne. Imetnikom MasterCard kartice se predlaga samo

blokada kartice in naročilo nove, nadomestne (menjava osebnega gesla pri MasterCard kartici ni možna in je potrebno naročiti novo). Če se imetnik plačilne kartice odloči za blokacijo (ne glede na vrsto kartice), se ga usmeri na klicni center Bankart (za blokacijo kartice je potrebno poklicati na tel. št.: 01 583 41 83, ki je navedena tudi na vsaki kartici), kjer blokacijo kartice opravijo takoj po prejemu klica. Omenjeni klicni center deluje vse dni v letu, 24 ur na dan, kar omogoča takojšnjo blokacijo plačilne kartice.

V OPP blokirajo plačilne kartice za katere obstaja sum zlorabe le v primeru, ko jim to v elektronskem sporočilu z nadaljnjimi navodili naroči pooblaščena kontaktna oseba banke. V tem primeru se imetnika kartice seznani tudi z višino stroškov iz tega naslova, po vsakokrat veljavnem ceniku banke X. V primeru, ko gre za večje število plačilnih kartic, ki so izpostavljene sumu zlorabe, se OPP glede izvedbe obveščanja naprej posvetuje s svojim nadrejenim. Če se kljub vsemu sprejme odločitev individualnega obveščanja imetnikov kartic, se tudi vsakič sproti določi časovni rok za izvedbo akcije.

V primerih, ko pride do suma zlorabe nekaj plačilnih kartic, se za zelo koristno in uporabno izkaže spletna aplikacija angl. *Web Cards*, ki je zgrajena na podoben način kot spletna aplikacija »Web Avtorizacijski logi«. Aplikacija Web Cards zagotavlja možnost direktnega vpogleda in spreminjanja avtorizacijskih parametrov kartic ter prikazuje osnovne podatke o imetniku kartice. Glavne funkcionalnosti aplikacije so:

- iskanje kartic po različnih kriterijih (ime in priimek, številka plačilne kartice PAN angl. *Primary Account Number* in ostalo),
- prikaz osnovnih podatkov o kartici in imetniku,
- podroben prikaz statusa posamezne kartice (SRM koda angl. *Simple Risk Management*) in
- spreminjanje SRM kode posamezne kartice.

Aplikacija omogoča spreminjanje SRM kode na sami kartici, s čimer se lahko prepreči njena nadaljnja uporaba na prodajnih mestih, ki niso podprta z EMV standardom, oziroma omogočajo uporabo kartic samo na podlagi magnetnega zapisa (večinoma v tujini, kjer še niso sprejeli EMV standarda). Poznamo več vrst SRM kod blokacij, s katerimi dosežemo različne vrste blokad na samih karticah. Lahko upoštevamo lokacijo blokade kartice (doma ali v tujini), vrsto tehnologije, ki se uporabi za transakcijo (magnetno ali čipno tehnologijo), način uporabe kartice (POS transakcije ali transakcije na bančnih avtomatih), ali pa kar kombinacijo vsega naštetega. V banki X se v primeru, ko pride do suma zlorabe nekaj plačilnih kartic, blokira SRM kodo št. 73, kar pomeni zavrnitev vseh tujih POS transakcij in transakcij na bančnih avtomatih, ki transakcije opravijo na podlagi magnetnega zapisa kartice in ne čipa. Aplikacija seveda omogoča tudi odstranitev blokade na kartici. Takšna vrsta blokade se ne izvede v primerih, ko se stranka odloči za blokacijo kartice in naročilo nove. Pomembno je tudi dejstvo, da lahko spletno aplikacijo uporabljajo samo tisti uporabniki, ki imajo ustrezne pravice in certifikat za dostop do Bankartovega spletnega vmesnika. Pravice se urejajo na ravni banke ter procesnega centra Bankart.

4.2 PROCES OZIROMA DELOVNA NAVODILA ZA RAVNANJE BANČNIH DELAVCEV V PRIMERU SUMA ZLORABE NA BANČNIH AVTOMATIH

Navodila vsebujejo priporočila za nadziranje bankomatov, preprečevanje zlorab na bankomatih in za ukrepanje v primeru odkritih zlorab na bankomatih. V prvi vrsti so namenjena bančnim delavcem, ki se ukvarjajo s kartičnim poslovanjem in z bankomati (vodje poslovnih enot, skrbniki bankomatov, skrbniki kartičnega modula v zaledju, pooblaščene kontaktne osebe banke, kontaktne osebe za varnost bankomatov) ter seveda vsem ostalim bančnim delavcem. Varnostni nadzor bankomatov temelji na:

- rednem varnostnem pregledovanju bankomatov, predvsem predela za vstavljanje kartic in predela ob in nad tipkovnico za vnos kode, da na bankomat ali v njegovi bližini niso dodatno nameščene nestandardne naprave in
- rednem obveščanju in ozaveščanju strank in bančnih delavcev o varnih postopkih pri rokovanju z bančnimi avtomati.

Naloga banke in bančnih delavcev je tudi redno obveščanje bančnih strank o tveganjih pri poslovanju s karticami in o načinih zmanjševanj teh tveganj.

4.2.1 Odkritje nameščene naprave

Če bančni delavec odkrije, da je na bančnem avtomatu nameščena nestandardna naprava, ukrepa na naslednje načine:

- takoj pokliče policijo na številko 113 ali na številko pristojne policijske postaje (odvisno od lokacije bančnega avtomata) ter jih obvesti o odkritju naprave,
- takoj obvesti 24-urno dežurno službo Bankarta, od katere zahteva prekinitev komunikacije s tem bančnim avtomatom (kar onemogoči njegovo nadaljnjo uporabo) ter jih seznani, da je policija o tem že obveščena,
- do prihoda policije takšen bančni avtomat zavaruje (s tem onemogoči njegovo nadaljnjo uporabo ter uničenje dokazov, v kolikor le-ti obstajajo) in ga z varne razdalje opazuje ter opažanja posreduje policistu,
- o dogodku ter o že izvedenih ukrepih obvesti pooblaščene kontaktne osebe banke X,
- pri pooblaščencu za varnost v banki X telefonsko in po elektronski pošti zahteva zavarovanje video posnetkov za obdobje, v katerem je predvidoma prišlo do namestitve naprave in se dogovori za pripravo posnetkov za pregled,
- pri pregledu video posnetkov, ki ga izvedeta skupaj s pooblaščenem za varnost takoj, ko je to mogoče, poizkušata ugotoviti čas, ko je bila na bankomatu izvajana zloraba, po potrebi oziroma na zahtevo se video posnetek preda policiji,
- z izvedenimi ukrepi seznani 24-urno dežurno službo Bankarta,
- po vzpostavitvi prvotnega stanja obvesti 24-urno dežurno službo Bankarta in zahteva aktiviranje bankomata,
- o dogodku napiše kratko poročilo in ga preda svojemu nadrejenemu in pooblaščencu za informacijsko varnost v banki.

4.2.2 Prejem obvestila o sumu namestitve nestandardne naprave na bančnem avtomatu banke X

Če bančni delavec prejme obvestilo o sumu namestitve nestandardne naprave na bančnem avtomatu v njegovi banki, ki ga lahko prejme s strani uporabnika bančnega avtomata, drugega bančnega delavca, procesnega centra Bankart, od policije ali od pooblaščene kontaktne osebe banke (ki je o tem obveščena s strani drugih kontaktnih pooblaščenih oseb bank), mora:

- takoj obvestiti 24-urno dežurno službo Bankarta ter zahtevati prekinitev komunikacije z bančnim avtomatom,
- osebno pregledati bančni avtomat in ugotoviti dejansko stanje in
- v kolikor obvestilo prejme s strani stranke ali drugega bančnega uslužbenca, le-tega prosi za:
  - osebno predstavitev (ime in priimek),
  - podatke o lokaciji sumljivega bankomata ter opažanja v zvezi z bankomatom (npr.: težko vstavljanje kartice v režo, namestitev sumljivih dodatkov na bankomatu) in
  - ga seznani s tem, da bo o sumu takoj obvestil policijo.

V kolikor bančni delavec ugotovi ali sumi, da je nameščena nestandardna naprava, ravna v skladu s poglavjem 4.2.1; če namestitev nestandardne naprave ni potrjena, pa o tem obvesti 24-urno dežurno službo Bankarta, kjer ponovno aktivirajo bančni avtomat. O dogodku napiše kratko poročilo in ga preda svojemu nadrejenemu in pooblaščencu za informacijsko varnost v banki.

4.2.3 Ostali varnostni incidenti in ukrepi

V primeru, da operater v 24-urni dežurni službi Bankarta zazna prekinitev delovanja bančnega avtomata v času, ko skrbnik bankomata ni dosegljiv (ponoči ali v nedelovnih dneh) in obstaja utemeljen sum, da je prekinitev posledica nasilnega dejanja na bankomatu (npr. odtujitev, vlom, fizično poškodovanje), o tem obvesti policijo in pooblaščeno kontaktno osebo banke lastnice bančnega avtomata. Pooblaščena kontaktna oseba, v izogib povzročitvi nadaljnje škode za banko in uporabnike, od dežurnega operaterja zahteva prekinitev komunikacije z bančnim avtomatom, dokler se okoliščine prekinitve normalnega delovanja ne raziščejo. Ko se okoliščine raziščejo in se ugotovi, da je delovanje bančnega avtomata zopet normalno in ne povzroča več nevarnosti, se zahteva ponovno vzpostavitev komunikacije z bančnim avtomatom.

4.3 STATISTIČNI PODATKI O ZLORABAH SKOZI LETA NA BANKI X

Kljub temu, da je težko pridobiti statistične podatke o zlorabah, saj gre za podatke zaupne narave (podatkov nam niso posredovali ne na Bankartu ne na ZBS), nam je uspelo pridobiti nekaj podatkov banke X (tudi na podlagi javno objavljenih letnih poročil).

4.3.1 Število zlorabljenih kartic

Iz tabele št. 13 je razvidno, da se je število blokiranih kartic v letu 2009 v primerjavi z letom 2008 v banki X povišalo. Razlago lahko iščemo v porastu števila izdanih kartic kot tudi v dejstvu, da je banka X namenila premalo pozornosti ter dodatnih ukrepov omenjeni problematiki s kartičnim poslovanjem. Tako je banka, kljub temu, da je bil odstotek zlorab na ves promet s karticami leta 2009 nekoliko manjši kot predhodno leto, pristopila k sprejetju ponudbe procesnega centra Bankarta, ki je v sodelovanju z MasterCardom programsko podprl sistem spremljanja poslovanja po plačilnih karticah, imenovan DMS (angl. *Dynamic Monitoring System*). Sistem deluje po principu vnaprej določenih kriterijev in omogoča izločanje transakcij, ki odstopajo od običajnih, ter oblikovanje poročil, ki so osnova za osebno kontaktiranje imetnikov plačilnih kartic. Leta 2010 se je v primerjavi z letom 2009 število blokiranih kartic zmanjšalo za 153, povišal pa se je odstotek zlorab na ves promet s karticami ter število zlorab. Za banko X je bil to dodaten argument za postopno uvedbo dodatne zaščite pri spletnem nakupovanju, in sicer standarda 3D Secure, ki deluje po principu avtentikacije (pred avtorizacijo transakcije se izvede dodatna varnostna kontrola imetnika kartice). V letu 2011 se je v primerjavi z letom 2010 tako število blokiranih kartic, kot tudi število zlorab povečalo (kljub zmanjšanju števila le-teh, kar je posledica odločitve banke X, da ukine neaktivne transakcijske račune in pripadajoče plačilne kartice). Po drugi strani pa se je odstotek zlorab na ves promet s karticami več kot prepolovil. Zato je šla banka X skupaj s procesnim centrom Bankart še korak naprej in pristopila k programski podpori, ki omogoča spremljanje poslovanja z vsemi plačilnimi karticami. Spremljanje deluje po načelu vnaprej določenih kriterijev, ki izločajo transakcije, ki odstopajo od običajnih. Kriteriji se lahko hitro in dokaj enostavno spremenijo, to pa omogoča sprotno spremljanje poslovanja s plačilnimi karticami ter hitro in ustrezno ukrepanje, ki je ključnega pomena pri zlorabah plačilnih kartic. Že v letu 2012 je število blokiranih kartic močno upadlo, kar je posledica spremljanja netipičnih transakcij ter predvsem uvedbe možnosti delnega blokiranja uporabe plačilnih kartic (s pomočjo spletne aplikacije angl. *Web Cards*). Banka s pomočjo spletne aplikacije angl. *Web Cards* blokira ustrezno SRM kodo na kartici in tako omogoča uporabo le-teh samo na prodajnih mestih, usklajenih z EMV standardom.

Iz tabele št. 13 ter s slike št. 2 lahko opazimo, da se število zlorab od leta 2009 povečuje. V letih 2011 in 2012 se število zlorab ni bistveno povečalo. To je dober pokazatelj, da je banka X s svojimi ukrepi na pravi poti k zmanjševanju števila zlorab oziroma vsaj ohranjanju na obstoječi ravni, in to kljub vedno večji priljubljenosti kartic kot plačilnega sredstva.

Tabela 13: Število in delež blokiranih in zlorabljenih kartic

Leto	Število vseh izdanih kartic	Število blokiranih kartic	% blokiranih kartic	Število zlorab	% zlorab na št. kartic	% zlorab na ves promet s karticami
2008	41.302	913	2,21	106	0,26	0,027
2009	45.228	1.142	2,53	100	0,22	0,023

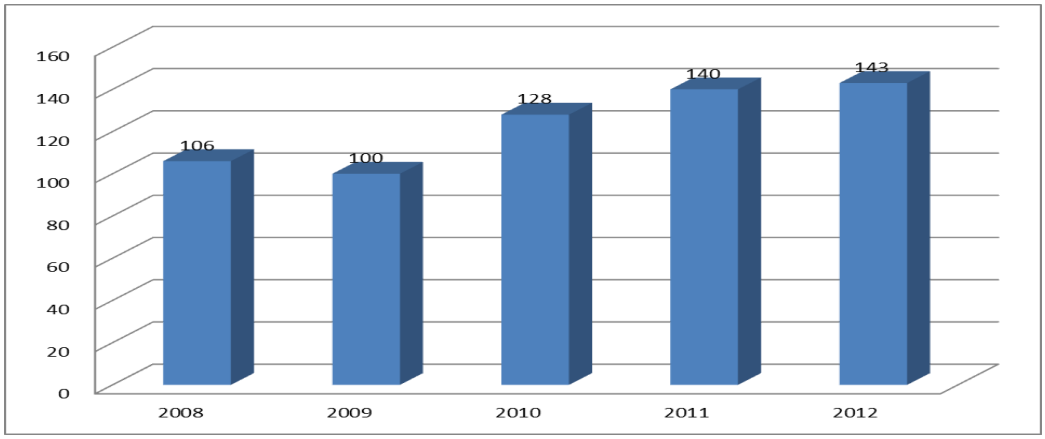
se nadaljuje

nadaljevanje

Leto	Število vseh izdanih kartic	Število blokiranih kartic	% blokiranih kartic	Število zlorab	% zlorab na št. kartic	% zlorab na ves promet s karticami
2010	47.695	989	2,07	128	0,27	0,046
2011	45.656	1.207	2,64	140	0,30	0,022
2012	47.085	832	1,77	143	0,30	0,020

Vir: Banka X, Letno poročilo banke X 2009, 2009, str. 24.; Banka X, Letno poročilo banke X 2010, 2010a, str. 26.; Banka X, Letno poročilo banke X 2011, 2011a, str. 34.; Banka X, Letno poročilo banke X 2012, 2012b, str. 35.

Slika 2: Število zlorab plačilnih kartic skozi leta



Vir: Banka X, Letno poročilo banke X 2009, 2009, str. 24.; Banka X, Letno poročilo banke X 2010, 2010a, str. 26.; Banka X, Letno poročilo banke X 2011, 2011a, str. 34.; Banka X, Letno poročilo banke X 2012, 2012b, str. 36.

Število reklamacij na podlagi zlorab plačilnih kartic

Tabela št. 14 prikazuje število reklamacij skozi leta, ki jih je prejel oddelek CBSI, v povezavi z zlorabljenimi plačilnimi karticami. Šlo je predvsem za reklamacije ob zlorabi plačilnih kartic, stroška blokacije plačilne kartice, zneska zlorabe in ostalega.

Tabela 14: Število prejetih reklamacij na temo zlorabe plačilnih kartic

Leto	2009	2010	2011	2012	Vsota
Št. reklamacij o zlorabah plačilnih kartic	125	42	38	58	263

Vir: Banka X, Interni statistični podatki banke X, 2013.

Število prejetih obvestil o sumu zlorabe

Iz tabele št. 15, ki prikazuje podrobno število prejetih obvestil o sumu zlorabe ter število plačilnih kartic, pri katerih obstaja sum zlorabe banke X v obdobju enega leta, je razvidno, da je na vsako prejeto obvestilo o sumu zlorabe približno pet plačilnih kartic, pri katerih obstaja sum

zlorabe oziroma so bile uporabljene na tistem prodajnem mestu, na katerem je bila nameščena naprava za snemanje magnetnega zapisa kartic.

Tabela 15: Število prejetih obvestil o sumu zlorabe ter število plačilnih kartic, pri katerih obstaja sum zlorabe

Obdobje	**Število prejetih obvestil o sumu zlorabe**	**Število plačilnih kartic, pri katerih obstaja sum zlorabe**
04. 04. - 31. 12. 2012	41	195
01. 01. - 04. 04. 2013	7	31
Skupaj v obdobju enega leta	48	226

Vir: Banka X, Interni statistični podatki banke X, 2013.

5 PREVENTIVNI UKREPI BANK, PROCESNIH CENTROV IN ZDRUŽENJ ZA PREPREČEVANJE ZLORAB PLAČILNIH KARTIC

Uporabniki storitev elektronskega bančništva so brez dvoma tisti, ki lahko sami največ naredijo za varnost poslovanja s svojimi kreditnimi in plačilnimi karticami. Zaradi tega je velik del dejavnosti tako bank, kakor tudi policije preko preventivnih ukrepov usmerjen na vlogo in ravnanje uporabnikov storitev. Čeprav je tehnologija elektronskega bančništva na videz in za računalniško podkovanega uporabnika sicer preprosta, pa je za opravljanje transakcije vseeno potrebno osvojiti nekaj znanja s področja uporabe tehnologij za elektronsko komuniciranje in poslovanje. Teh znanj največkrat niso vešči ravno starejši ljudje, ki pogosto tudi zaradi tega in nepazljivosti pri ravnanju in opravljanju storitev elektronskega bančništva postanejo žrtve različnih oblik zlorab. [...] Z informatizacijo bančnega poslovanja so finančne inštitucije skoraj v celoti prešle na elektronsko poslovanje in ponudile uporabnikom kopico novih storitev in instrumentov, za njihovo uporabo pa je potrebno že določeno znanje (Lamberger, 2011, str. 120).

Zavedati pa se moramo, da zlorabam niso izpostavljeni samo starejši ljudje, ampak tudi vsak povprečen uporabnik, saj so nepridipravi zelo vešči in tehnično dobro podkovani. In ravno zato je s strani bank, procesnih centov in združenj, kot tudi organov zakona, pomembno preventivno ukrepanje, s čimer se poskuša kar se da zmanjšati finančno izgubo vseh sodelujočih.

5.1 PRIPOROČILA BANKARTA, ZBS IN BANK ZA VARNO RABO PLAČILNIH KARTIC

Kartico je treba razumeti enako kot denar, zato je z njo potrebno ravnati odgovorno in previdno. ZBS in Bankart sta pripravila priporočila za rokovanje s kartico (Osnovna pravila za varno poslovanje s karticami, 2013):

Splošna pravila:

- Ponovno se seznanite s splošnimi pogoji poslovanja, ki veljajo za vašo kartico.
- Novo plačilno kartico ob prejemu takoj podpišite, saj je veljavna le podpisana kartica. Staro, neveljavno ali preklicano kartico takoj uničite, oziroma jo takoj razrežite.

- Kartice ne hranite na soncu ali blizu drugih toplotnih virov, elektromagnetnega sevanja in drugih škodljivih vplivov oziroma virov, ker se lahko poškoduje in postane neuporabna.
- S kartico ravnajte skrbno, imejte jo vedno pri sebi in je ne puščajte v avtu, garderobi ali kje drugje. Kadar plačujete s kartico, je nikoli ne izpustite izpred oči. V restavraciji naj natakar uporabi prenosni POS terminal ali pa ga sami pospremite do plačilnega mesta.
- PIN številko si takoj po prejemu zapomnite in uničite dopis, s katerim ste jo prejeli.
- Osebne PIN številke nikakor ne imejte zapisane nikjer skupaj s kartico. Tudi doma ne.
- Kartica je osebna, nihče drug z njo ne sme opravljati nobenih storitev.
- Številka kartice in njej pripadajoči podatki so tajni in unikatni, zato jih ne povejte vsakomur, ki vas povpraša po teh podatkih.
- Ne verjemite elektronskim, telefonskim ali drugim sporočilom, četudi navidezno prihajajo od vaše banke, s katerimi vas obveščajo o zlorabi vaše kartice in vas pozivajo, da poveste podatke o svoji kartici ali da jih vpišete v spletne, tako imenovane varnostne obrazce. O takem dogodku obvestite svojo banko ali hranilnico in z njo preverite vsebino sporočila.
- Redno spremljajte promet na kartici prek spletne banke. Če opazite transakcije, ki jih niste opravili, o tem takoj obvestite svojo banko ali hranilnico.

Poslovanje na prodajnih mestih:

- Pri plačevanju kartice nikoli ne izpustite iz svojega vidnega polja in nadzirajte celoten postopek plačevanja.
- Pred vnosom osebne PIN številke oziroma pred podpisom potrdila obvezno preverite znesek plačila.
- V postopku plačevanja na prodajnem mestu pazite, da nihče ne vidi vaše osebne PIN številke. Ko opravljate katero koli storitev (še posebej z uporabo bančnega avtomata) pazite, da nihče ne vidi vaše osebne PIN številke, ki ste jo vtipkali in da so čakajoči za vami dovolj oddaljeni od vas. Če kdo stoji preblizu, ga prosite, naj se odmakne.
- Bodite pozorni, da oseba, ki vam zaračunava blago ali storitev, kartico avtorizira oziroma jo potegne skozi POS terminal samo enkrat. V primeru neuspešne avtorizacije zahtevajte potrdilo o neuspešno opravljenem postopku.
- Potrdila o že opravljenih nakupih po navadi vsebujejo dovolj podatkov o kartici, zato stara potrdila uničite.
- Preden zavržete potrdila o nakupih, natančno preverite vse izpiske porabe. Le s primerjavo izpiska porabe s potrdilom o nakupu lahko ugotovite svojo dejansko porabo.
- Na prodajnih mestih ne podpisujte potrdil, ki niso namenjena takojšnjemu plačilu blaga ali storitve in so napisana z vnaprejšnjimi datumi ali so celo prazna.

Spletno nakupovanje:

- Na spletnih straneh ne vpisujte številke kartice povsod, kjer jo od vas zahtevajo, temveč le takrat, ko ste se že odločili za nakup in dejansko želite plačati s kartico.
- Prek spleta plačujte le tistim ponudnikom, za katere veste, da so verodostojni, varni in imajo zagotovljene varnostne nastavitve na svojih spletnih straneh.

- Obvezno poskrbite, da bo tudi vaš računalnik dobro zaščiten pred vdori, zlorabami in zlonamerno programsko opremo.

Uporaba bančnega avtomata:

- Med uporabo bančnega avtomata nihče ne sme videti vaše osebne PIN številke. Pri vpisovanju osebne PIN številke priporočamo, da z roko zastrete tipkovnico. Če kdo stoji preblizu, ga prosite, naj se odmakne.
- Bančne avtomate uporabljajte sami. Če jih ne znate uporabljati, ne sprejemajte pomoči mimoidočega, temveč se raje o uporabi poučite v svoji banki ali hranilnici.
- Kartico uporabljajte na tistih avtomatih, ki stojijo na obljudenem in dobro osvetljenem mestu.
- Če na bančnem avtomatu zaznate kakršna koli odstopanja od običajnega delovanja (npr. kartico težje vložite v avtomat, na avtomatu so naprave ali stvari, ki jih običajno ni, neobičajna postavitev kamer, neobičajna reža, v katero se vlaga kartica, …), vzemite kartico in zapustite bančni avtomat ter uporabite drugega. O tem čim prej obvestite banko ali hranilnico na telefonsko številko, ki je zapisana na kartici, in policijo na številko 113.
- Če so bančni avtomati nameščeni v zaprtih prostorih, do katerih lahko vstopate le skozi vrata s potegom kartice, vedite, da ob tem nikoli ni treba vtipkati osebne PIN številke. Če je na vratih naprava, ki od vas zahteva tipkanje osebne PIN številke, tega ne storite!
- V primeru, da vam bančni avtomat ne vrne kartice (zaradi ovire, nameščene na reži za sprejem kartice), ob ali na njem pa je prilepljeno navodilo, da ponovno vtipkajte osebno PIN številko, tega ne storite. Enako velja, če vam ponoven vnos osebne PIN številke predlaga oseba, ki se nahaja v bližini in se predstavlja za bančnega delavca. V obeh primerih takoj obvestite najbližjo enoto banke ali hranilnice in policijo na 113.
- V primeru, da vam bančni avtomat navkljub odobreni storitvi ne izplača gotovine, takoj preverite stanje na svojem računu in se oglasite v najbližji poslovalnici banke ali hranilnice.

Varni na potovanju:

- Če potujete v tujino, je dobro razpolagati z več različnimi karticami.
- Pred potovanjem preverite veljavnost kartice in razpoložljiv limit.
- Kopirajte svojo kartico in potni list ter kopije hranite ločeno in varno.
- Kartice in gotovino hranite ločeno, na ta način v primeru kraje ne boste ob vse.
- V gneči imejte torbico ali denarnico tesno ob sebi.
- V hotelskih sobah ali apartmajih uporabljajte sefe za hranjenje dragocenosti, gotovine in kartic.
- Pri plačevanju s kartico pred podpisom ali vnosom osebne PIN številke preverite informacije na računu, slipu ali POS terminalu.

Preklici, izgube, kraje:

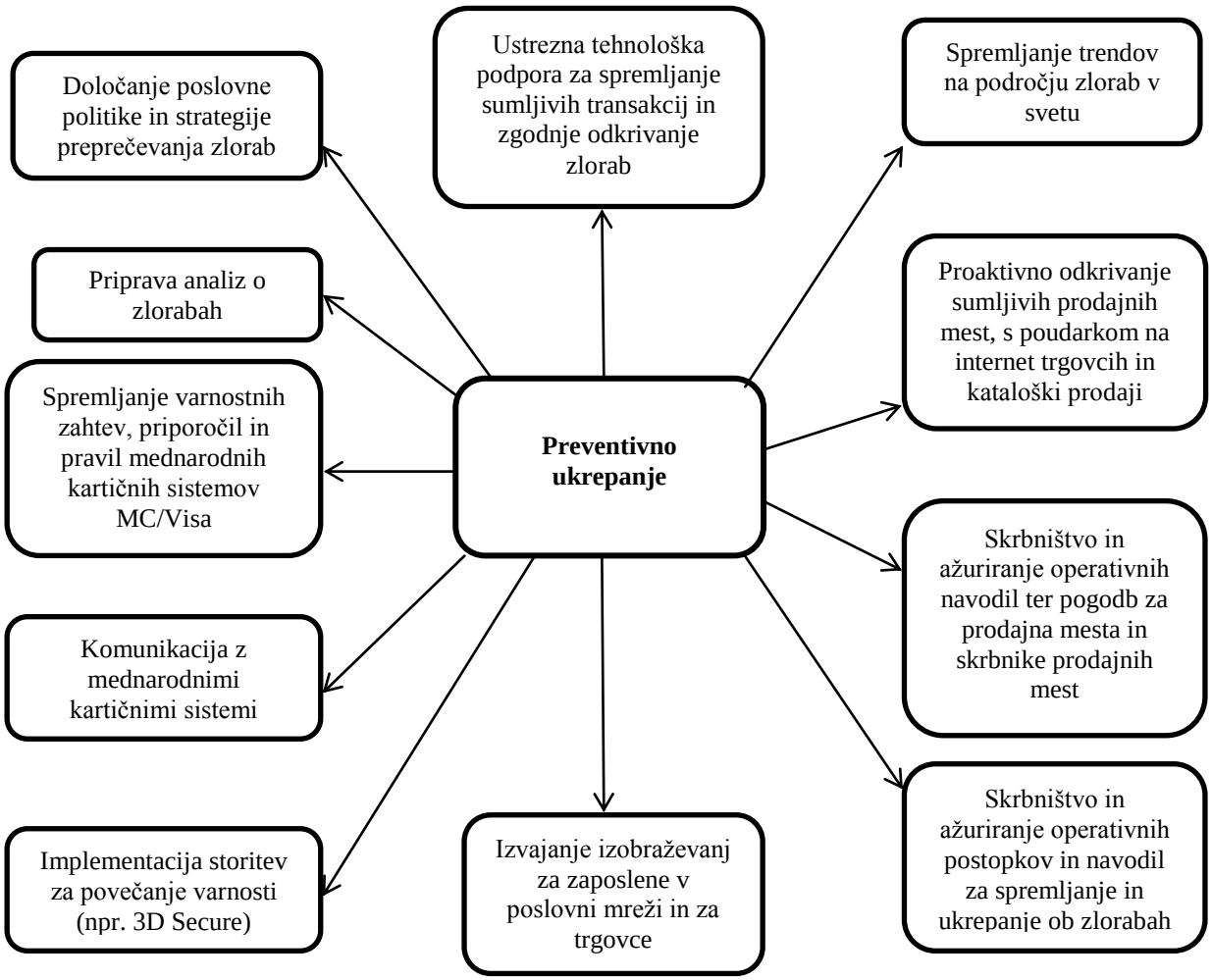
- Zapišite si telefonsko številko, ki ste jo prejeli od izdajatelja kartice in na katero lahko 24 ur na dan, 365 dni na leto pokličete in takoj prijavite izgubo ali krajo kartice.

- Prijavo preklica, izgube ali kraje opravite takoj. Le tako bo vaša kartica blokirana in s tem zmanjšana možnost zlorabe.
- Sum kraje kartice obvezno prijavite tudi najbližji policijski postaji. Enako storite tudi, če ste v tujini.

Seveda pa na spletnih straneh Bankarta, ZBS, Policije, Europola in ostalih najdemo še veliko več navodil, priporočil in osnovnih informacij. Na spletnih straneh Bankarta zasledimo tudi video posnetek glede same uporabe plačilnih kartic na bančnih avtomatih.

Priporočila bank se ne razlikujejo od priporočil Bankarta in ZBS, kar je popolnoma razumljivo, saj le-ti med seboj tesno sodelujejo ter jih skupaj pišejo in dopolnjujejo. Največjo težavo za banke kljub vsem naporom predstavljajo sami uporabniki, ki žal še vedno ne upoštevajo (vsaj ne v zadostni meri) priporočil za varno rabo plačilnih kartic. Vemo, da se zlorab ne da popolnoma preprečiti, zato je za banke pomembno preventivno ukrepanje, ki ga lahko strnemo v spodnji miselni vzorec:

Slika 3: Miselni vzorec preventivnih ukrepov bank za preprečevanje zlorab plačilnih kartic



Vir: A. Mejač Krassnig, Poslovni vidiki banke do imetnikov in trgovcev, 2012, str. 8.

Preventivni ukrepi so zelo pomembni, vendar banke vse odgovornosti ne morejo prenesti na uporabnike oziroma imetnike, zato morajo zagotoviti tudi konstantno osveščanje ter izobraževanje osebja, trgovcev ter nuditi ustrezno varovanje opreme, nameniti veliko pozornosti izbiri dobaviteljev programske opreme in izvajalcev raznih storitev, kot tudi redno izobraževati svoje zaposlene. Le na tak način bodo banke dodobra obvladovale tveganja, ki se jim kot izdajateljice plačilnih kartic izpostavljajo. Zavedati se morajo namreč, da je za čim boljše obvladovanje tveganj pomembno, da sledijo varnostnim standardom, ki jih postavijo kartični sistemi ter jih istočasno s svojimi aktivnostmi celo dopolnjujejo oziroma nadgrajujejo ter s tem zmanjšujejo število zlorab, kar konec koncev pripelje do minimiziranja finančne izgube ter večjega zaupanja strank.

SKLEP

V bančništvu smo priča hitremu, za nekatere uporabnike osnovnih bančnih storitev, celo prehitremu razvoju. Skoraj vsak dan lahko v medijih zasledimo razne novosti, ki jih banke ponujajo svojim komitentom, kar je odraz hude konkurenčne tekme za vsako stranko ter dejstva, da želijo banke zadostiti, ne samo zakonodaji in predpisom oziroma priporočilom, ampak tudi željam svojih komitentov. Nič drugače ni s plačilnimi karticami, ki so zaradi svoje priročnosti in enostavne uporabe vedno bolj priljubljene ter uporabljane med ljudmi. Imetnikom omogočajo enostavno in hitro plačevanje v trgovinah, nakupe prek spleta, dostop do denarja je s pomočjo bančnih avtomatov omogočen skozi celo leto, za marsikoga predstavljajo tudi statusni simbol, omogočajo pa tudi veliko ostalih ugodnosti in koristi. Banke kot izdajateljice pa seveda vidijo svoje koristi predvsem z vidika pridobivanja provizij iz naslova plačila blaga in storitev, provizij za dvige gotovine, drugih prihodkov (kot recimo kreditne obresti, članarine in ostalo), srečujejo se tudi z lojalnostjo strank in možnostjo navzkrižne ponudbe, kot tudi z nižjimi stroški poslovanja v primerjavi z gotovino ali izdajanjem čekov.

Poznamo veliko vrst plačilnih kartic in lahko jih razdelimo po več kriterijih. Med pomembnejšimi je zagotovo delitev glede na način plačila, kamor sodijo debetne, kreditne, kreditne z odloženim plačilom in predplačilne kartice, v velikem porastu pa so v zadnjem času tudi kartice zvestobe oziroma lojalnosti, ki jih ponujajo razni trgovci in drogerije.

Lahko bi rekli, da ima vsaka stvar tako svoje prednosti kot tudi slabosti. Tako je tudi pri plačilnih karticah, katerih glavna slabost je, da nepridipravom omogočajo veliko možnosti oziroma načinov zlorab. O zlorabi govorimo takrat, ko je uporaba plačilne kartice opravljena s strani nepooblaščene tretje osebe. Najpogostejša načina zlorabe sta spletne prevare in kopiranje magnetnega zapisa s plačilne kartice brez vednosti in soglasja imetnika kartice.

Za banke kot izdajateljice plačilnih kartic je pomembno, da upoštevajo navodila oziroma priporočila tako procesnih centrov kot ZBS, ter jih s svojimi internimi procesi in navodili še nadgradijo, s čimer dodatno zmanjšajo tveganja, ki so jim kot izdajateljice izpostavljene. Za čim boljšo in hitrejšo odzivnost v primerih zlorab plačilnih kartic je zelo pomembna homogenost vseh sodelujočih v kartičnem procesu ter seveda ustrezno sodelovanje z organi pregona. Z

namenom minimiziranja finančne škode ter zmanjšanja zlorab je za banke v prvi fazi pomembno preventivno ukrepanje. Ker pa vemo, da se zlorab v celoti ne da preprečiti, je pomembno tudi ustrezno incidentno ukrepanje bank v primerih, ko do zlorab že pride. Incidentno ukrepanje zahteva od izdajatelja hitro ukrepanje v smislu blokacije kartic, obveščanja imetnikov in spremljanja transakcij. Ravno tako zahteva sprejemanje ustreznih odločitev o vrsti ukrepov glede na vrsto zlorabe ter ažurno obveščanje pristojnih organizacijskih enot o aktivnostih za ukrepe; ob tem morajo imeti pooblaščene kontaktne osebe bank ustrezna pooblastila za samostojno odločanje in ukrepanje. Zelo pomembno je tudi samo sodelovanje z zunanjimi institucijami, kot so procesni center, organi pregona in ZBS, kot tudi dnevno spremljanje obvestil o zlorabah s strani kartičnih sistemov. Ukrepanje v primeru incidenta mora biti omogočeno vse dni skozi celo leto, saj so zlorabe nepredvidljive. Naj omenimo še, da sta leti 1974 (začetek pametnih kartic) in 1994 (EMV standard - trije največji svetovni izdajatelji kartic Eurocard, MasterCard in Visa so se dogovorili za enoten nastop na področju uvajanja tehnologije pametnih kartic) zagotovo zelo pomembna mejnika z vidika varnosti plačilnih kartic.

Največjo težavo z vidika zlorabe plačilnih kartic s kopiranjem magnetnega zapisa predstavlja dejstvo, da je po svetu še kar nekaj držav, ki niso sprejele EMV standarda. V teh državah se izvede največ prevar s ponarejenimi karticami, saj omogočajo uporabo samo magnetnega zapisa in ne čipne tehnologije. Vendar pa lahko v teh dneh na spletnih straneh bank zasledimo obvestilo, da so le-te omejile poslovanje za gotovinske dvige na bankomatih v nekaterih državah oziroma regijah, ki ne upoštevajo vseh mednarodnih varnostnih standardov bankomatskega poslovanja, s čimer želijo še dodatno zmanjšati število prevar.

Za varno uporabo plačilnih kartic lahko, z upoštevanjem navodil, priporočil ter previdno rabo, največ naredijo prav imetniki sami. Potrebno se je zavedati, da so plačilne kartice v bistvu denar in ne zgolj kos plastike, zato je potrebno biti ob uporabi le-teh skrajno previden in odgovoren. Le na takšen način lahko zmanjšamo možnost zlorabe. Vsekakor pa je za zmanjševanje zlorab pomembno tudi učinkovito in hitro ukrepanje organov pregona ter procesnih centrov ter tudi skrb izdajateljev plačilnih kartic za ustrezno ozaveščenost imetnikov o varni uporabi plačilnih kartic. Zmanjšanje zlorab bo seveda možno samo ob sočasnem sodelovanju in upoštevanju varnostnih priporočil ter preventivnih ukrepov vseh sodelujočih pri kartičnem poslovanju. Znano je, da zlorab kartic ne moremo v celoti preprečiti, lahko pa škodo, ki bi nastala iz tega naslova, s hitrim in primernim ukrepanjem vsaj zmanjšamo na čim nižjo raven.

LITERATURA IN VIRI

1. *Activa Maestro*. Najdeno 30. maja 2013 na spletnem naslovu http://www.sberbank.si/prebivalstvo/placilne-kartice/activa-maestro.aspx
2. Andrić, S. (2010). *Sodobno brezgotovinsko plačevanje: analiza vrednosti za uporabnika na primeru plačilnih kartic in storitve Moneta* (magistrsko delo). Ljubljana: Ekonomska fakulteta.
3. Banka Slovenije. (2013). Bilten. *Bilten Banke Slovenije*. (Št. 1, januar 2013). Ljubljana: Banka Slovenije.
4. Banka X. (2009). Letno poročilo Banke X. Ljubljana: Banka X.
5. Banka X. (2010a). Letno poročilo Banke X. Ljubljana: Banka X.
6. Banka X. (2010b). *Protokol kartičnega poslovanja* (interno gradivo). Ljubljana: Banka X.
7. Banka X. (2011a). Letno poročilo Banke X. Ljubljana: Banka X.
8. Banka X. (2011b). *Varnostni nadzor bankomatov* (interno gradivo). Ljubljana: Banka X.
9. Banka X. (2012a). *Blokacije kartic in prodajnih mest* (interno gradivo). Ljubljana: Banka X.
10. Banka X. (2012b). Letno poročilo Banke X. Ljubljana: Banka X.
11. Banka X. (2012c). *Preprečevanje zlorab po plačilnih karticah, prejem in posredovanje sporočil, ter ukrepanje* (interno gradivo). Ljubljana: Banka X.
12. Banka X. (2012d). *Prevzem in hranjenje plačilnih kartic in gesel* (interno gradivo). Ljubljana: Banka X.
13. Banka X. (2012e). *Zlorabe plačilnih kartic in ukrepanje v OPP* (interno gradivo). Ljubljana: Banka X.
14. Banka X. (2013). *Interni statistični podatki* (interno gradivo). Ljubljana: Banka X.
15. *Be smart with your card.* Najdeno 30. maja 2013 na spletnem naslovu https://www.europol.europa.eu/sites/default/files/be_smart_with_your_card_v4.pdf
16. Bertoncelj, B. (2012). *Tveganje pri poslovanju z bančnim avtomatom.* Ljubljana: Združenje bank Slovenije.
17. *Card Fraud.* Najdeno 17. aprila 2013 na spletnem naslovu http://www.financialfraudaction.org.uk/Financial-card-fraud.asp
18. *Cene in obrestne mere*. Najdeno 31. maja 2013 na spletnem naslovu http://www.abanka.si/cene-in-obrestne-mere/
19. *Cenik osebne finance*. Najdeno 31. maja 2013 na spletnem naslovu http://www.pbs.si/si/cenik_osebne_finance.wlgt
20. *Cenik poslovanja*. Najdeno 31. maja 2013 na spletnem naslovu http://www.factorb.si/FB_SI,,osebne_finance/cenik_poslovanja
21. *Cenik storitev*. Najdeno 31. maja 2013a na spletnem naslovu http://www.nkbm.si/cenik-storitev
22. *Ceniki storitev*. Najdeno 31. maja 2013b na spletnem naslovu http://www.sberbank.si/sl/pripomocki/cenik-storitev.aspx
23. *Ceniki*. Najdeno 31. maja 2013a na spletnem naslovu http://www.banka-celje.si/ostalo/cenik
24. *Ceniki*. Najdeno 31. maja 2013b na spletnem naslovu http://www.hypo-alpe-adria.si/sl/content/ceniki
25. *Ceniki*. Najdeno 31. maja 2013c na spletnem naslovu http://www.skb.si/osebne-finance/ceniki
26. *Credit Card Skimming Alert*. Najdeno 15. aprila 2013 na spletnem naslovu http://www.docstoc.com/docs/2326728/Credit-Card-Skimming-Alert
27. *Credit Card Skimming Devices*. Najdeno 15. aprila 2013 na spletnem naslovu http://creditcardskimming.blogspot.com/p/cc-reader-writer.html
28. Drakulič, I. (2006a). Vse bolj priljubljena plastika. *Glas gospodarstva.* Najdeno 25. marca 2013 na spletnem naslovu http://www.gzs.si/slo/30554

29. Drakulič, I. (2006b). Partnerske kartice – korist za vse. *Glas gospodarstva*. Najdeno 25. marca 2013 na spletnem naslovu http://www.gzs.si/slo/30555
30. European Central Bank. (2012). Report on card fraud. Najdeno 17. aprila 2013 na spletnem naslovu http://www.ecb.int/pub/pdf/other/cardfraudreport201207en.pdf
31. Felc, M. (2012). Goljufi stalno iščejo pomanjkljivosti. *Nedelo*. Najdeno 16. aprila 2013 na spletnem naslovu http://www.delo.si/novice/slovenija/goljufi-stalno-iscejo-pomanjkljivosti.html
32. Gracer, D. (b.l.). Skimming naprave v Sloveniji. Najdeno 20. marca 2013 na spletnem naslovu http://www.fvv.uni-mb.si/konferencaIV/zbornik/Gracer.pdf
33. Gradišar, M., & Lamberger, I. (2011). Celovit sistem zaščite elektronskih plačilnih sistemov pred zlorabami. *Revija za denarništvo in bančništvo, 60* (*3*), 13-20.
34. *Hranilnica Vipava d.d.*. Najdeno 30. maja 2013 na spletnem naslovu http://www.hranilnica-vipava.si/
35. *Izvleček iz tarife poslovanja s prebivalstvom*. Najdeno 31. maja 2013 na spletnem naslovu http://www.unicreditbank.si/sl/Prebivalstvo/Uporabno/Izvlecek_iz_tarife
36. Janžekovič, M. (2007). *Sistemi plačilnih kartic s poudarkom na sistemu Activa* (diplomsko delo). Maribor: Ekonomsko-poslovna fakulteta.
37. Jurišić, A., & Tonejc, J. (2001). Pametne kartice in varnost. *Monitor*, str. 66-75.
38. *Kaj je »3-D Secure«?*. Najdeno 27. marca 2013 na spletnem naslovu http://www.nlb.si/3d-secure
39. *Kartice in Moneta*. Najdeno 30. maja 2013 na spletnem naslovu http://www.nkbm.si/kartice-in-moneta
40. *Kartice ugodnosti*. Najdeno 22. marca 2013 na spletnem naslovu http://www.denarnisupermarket.com/?pt=pkartice&k_pod=8
41. *Kartice*. Najdeno 30. maja 2013a na spletnem naslovu http://www.abanka.si/kartice/
42. *Kartice*. Najdeno 30. maja 2013b na spletnem naslovu http://www.banka-celje.si/osebne-finance/kartice
43. *Kartice*. Najdeno 30. maja 2013c na spletnem naslovu http://www.factorb.si/FB_SI,,osebne_finance/kartice
44. *Kartice*. Najdeno 30. maja 2013d na spletnem naslovu http://www.hypo-alpe-adria.si/sl/content/kartice-0
45. *Kartice*. Najdeno 30. maja 2013e na spletnem naslovu http://www.raiffeisen.si/kartice/
46. *Kartice*. Najdeno 30. maja 2013f na spletnem naslovu http://www.skb.si/osebne-finance/kartice
47. *Kartice*. Najdeno 30. maja 2013g na spletnem naslovu http://www.unicreditbank.si/sl/Prebivalstvo/Kartice
48. Krivec, V. (2007). Plastična doba. *Mag*. Najdeno 21. marca 2013 na spletnem naslovu http://www.delo.si/arhiv/plasticna-doba.html
49. Kutin, B. (2011). Kartice zvestobe – vohuni v nakupovalnem vozičku? Najdeno 23. marca 2013 na spletnem naslovu http://www.zps.si/za-medije/izjave-za-javnost-2011/kartice-zvestobe-vohuni-v-nakupovalnem-vozicku.html?Itemid=687
50. Lamberger, I. (2011). *Model zaščite elektronskih plačilnih sistemov pred zlorabami* (doktorska disertacija). Ljubljana: Ekonomska fakulteta.
51. Lešnik, T. (2012). *Kartično poslovanje in trendi.* Ljubljana: Združenje bank Slovenije.
52. Logar, R. (1998). *Plačilni sistemi: kaj je dobro vedeti o njih.* Ljubljana: Slovenski inštitut za revizijo.
53. Magnetic stripe card. (b.l.). *V Wikipedia*. Najdeno 23. marca 2013 na spletni strani http://en.wikipedia.org/wiki/Magnetic_stripe_card
54. Mejač Krassnig, A. (2012). *Poslovni vidiki banke do imetnikov in trgovcev.* Ljubljana: Združenje bank Slovenije.

55. *Navadna kartica*. Najdeno 30. maja 2013 na spletnem naslovu http://www.delavska-hranilnica.si/DH,,osebne_finance,kartica_mastercard,navadna_kartica.htm
56. *Neue Betrugsmethode an Geldautomaten.* Najdeno 16. aprila 2013 na spletnem naslovu http://www.ruhrnachrichten.de/bilder/fotostrecken/cme102638,2244124
57. Novak, P. (2009). *Elektronsko bančništvo in kartično poslovanje* (diplomsko delo). Maribor: Ekonomsko-poslovna fakulteta.
58. *Obrestne mere*. Najdeno 31. maja 2013 na spletnem naslovu http://www.sparkasse.si/obrestne-mere
59. Odar, M. (2000). Kreditne (zaupanjske) kartice. *IKS: revija za računovodstvo in finance, 27* (*9*), 93-107.
60. *Osnovna pravila varne rabe kartic*. Najdeno 2. junija 2013 na spletnem naslovu http://www.zbs-giz.si/zdruzenje-bank.asp?StructureId=887
61. *Osnovna pravila za varno poslovanje s karticami.* Najdeno 2. junija 2013 na spletnem naslovu http://www.bankart.si/si/ponudba/procesiranje_prometa_placilnih_kartic/navodila_ba/
62. *Paketni računi kartice*. Najdeno 30. maja 2013 na spletnem naslovu http://www.sparkasse.si/paketni-racun-kartice
63. *Pametna kartica ponuja več.* Najdeno 25. marca 2013 na spletnem naslovu http://www.activa.si/pametnaKartica/?content=smart-card
64. Pharming. (2013). V *Wikipedia*. Najdeno 25. marca na spletni strani http://en.wikipedia.org/wiki/Pharming
65. *Plačilne in kreditne kartice*. Najdeno 30. maja 2013 na spletnem naslovu http://www.lon.si/si/osebne_finance/placilne_in_kreditne_kartice.htm
66. Plačilne kartice. (b.l.). *V Moj denar*. Najdeno 21. marca 2013 na spletnem naslovu http://www.mojdenar.com/BANKE/plac_kart_splosno.asp
67. *Plačilne kartice*. Najdeno 30. maja 2013a na spletnem naslovu http://www.banka-koper.si/Fizicne_osebe/Placilne_kartice
68. *Plačilne kartice*. Najdeno 30. maja 2013b na spletnem naslovu http://www.bksbank.si/BKSWebp/BKS/bks_si/Fizicne_osebe/Plailne_storitve/Placilne_kartice/index.jsp
69. *Plačilne kartice*. Najdeno 30. maja 2013c na spletnem naslovu http://www.dbs.si/
70. *Plačilne kartice*. Najdeno 30. maja 2013d na spletnem naslovu http://www.gbkr.si/osebne-finance/placilne-kartice/
71. *Plačilne kartice*. Najdeno 30. maja 2013e na spletnem naslovu http://www.nlb.si/placilne-kartice
72. *Plačilne kartice*. Najdeno 30. maja 2013f na spletnem naslovu http://www.pbs.si/si/placilne_kartice.wlgt
73. *Plačilne kartice*. Najdeno 30. maja 2013g na spletnem naslovu http://www.probanka.si/kategorije/969/Placilne-kartice
74. Policija. (2010). Poročilo o delu Policije za leto 2010. Ljubljana: Policija.
75. Policija. (2011). Poročilo o delu Policije za leto 2011. Ljubljana: Policija.
76. Policija. (2012). Poročilo o delu Policije za prvo polletje 2012. Ljubljana: Policija.
77. *Prevara na bančnih avtomatih (Skimming)*. Najdeno 15. aprila 2013 na spletnem naslovu http://web-center.si/varnostna-obvestila/196-prevara-na-bancnih-avtomatih
78. *Rear of an ATM card skimming device captured by Perth police 6 December 2012.* Najdeno 15. aprila 2013 na spletnem naslovu http://www.abc.net.au/news/2012-12-06/atm-skimmer-psjpg/4413010
79. Secure Electronic Transaction. (2013). V *Wikipedia*. Najdeno 26. marca 2013 na spletni strani http://en.wikipedia.org/wiki/Secure_Electronic_Transaction
80. *Smard cards*. Najdeno 24. marca 2013 na spletnem naslovu http://kgb.scriptmania.com/smartcards/vortrag.htm

81. Spletno ribarjenje. (2013). V *Wikipedia*. Najdeno 24. marca 2013 na spletni strani https://sl.wikipedia.org/wiki/Spletno_ribarjenje
82. *Stroški in obrestne mere*. Najdeno 31. maja 2013 na spletnem naslovu http://www.nlb.si/obrestne-mere
83. Šimunovič, K. (2008). *Sistemi kartičnega poslovanja in njihova varnost* (diplomsko delo). Maribor: Ekonomsko-poslovna fakulteta.
84. *Tarife – Občani*. Najdeno 31. maja 2013 na spletnem naslovu http://www.delavska-hranilnica.si/DH,,razno,tarife,obcani.htm
85. *Tarife banke*. Najdeno 31. maja 2013 na spletnem naslovu http://www.banka-koper.si/Fizicne_osebe/Pripomocki/Tarifa_banke
86. *Tarife in obrestne mere*. Najdeno 31. maja 2013 na spletnem naslovu http://www.dbs.si/orodja/obrestnemere/tarife.asp?MapaID=427
87. *Tarife nadomestila*. Najdeno 31. maja 2013 na spletnem naslovu http://www.gbkr.si/osebne-finance/pripomocki/tarifa-nadomestil/
88. *Tarife plačil*. Najdeno 31. maja 2013 na spletnem naslovu http://www.hranilnica-vipava.si/page7.html
89. *Tarife*. Najdeno 31. maja 2013a na spletnem naslovu http://www.lon.si/si/pripomocki/tarife.htm
90. *Tarife*. Najdeno 31. maja 2013b na spletnem naslovu http://www.probanka.si/tarife/1245
91. *Tarife*. Najdeno 31. maja 2013c na spletnem naslovu http://www.raiffeisen.si/ceniki_in_tecaji/tarife/
92. Trstenjak, M. (2003). Zlorabe plačilnih kartic. *Revija Kapital*. Najdeno 18. marca 2013 na spletnem naslovu http://www.revijakapital.com/kapital/poslovnefinance.php?idclanka=1074&oznaci=Zlorabe+pla%E8ilne+kartice
93. Turk, I. (2004). *Pojmovnik računovodstva financ in revizije.* Ljubljana: Zveza računovodij, finančnikov in revizorjev Slovenije.
94. *Upravljane in servis POS-terminalov*. Najdeno 3. aprila 2013 na spletnem naslovu http://www.bankart.si/si/ponudba/upravljanje_in_servis_terminalov_pos/
95. *Vezane vloge depoziti*. Najdeno 31. maja 2013 na spletnem naslovu http://www.bksbank.si/BKSWebp/BKS/bks_si/Fizicne_osebe/Vrarcevanje/Vezane_vloge__depoziti/index.jsp#tab5
96. Walters, C. (2009). How ATM card skimming works. Najdeno 15. aprila 2013 na spletnem naslovu http://www.crikey.com.au/2009/03/30/how-atm-card-skimming-works/
97. *Zgodovina pametnih kartic*. Najdeno 25. marca 2013 na spletnem naslovu http://www.activa.si/pametnaKartica/zgodovina.asp

PRILOGE

KAZALO PRILOG

Priloga 1: Prenosne skimming naprave

Slika 1: Prenosna skimming naprava

Vir: Credit Card Skimming alert, 2013.

Slika 2: Snemalno zapisovalna naprava

Vir: Credit Card Skimming Devices, 2013.

Priloga 2: Čitalec in kamera na bančnem avtomatu ter prirejena številčnica

Slika 3: Čitalec kartice in kamera na bančnem avtomatu

Vir: Prevara na bančnih avtomatih (Skimming), 2011.

Slika 4 Prirejena številčnica na bančnem avtomatu

Vir: Prevara na bančnih avtomatih (Skimming), 2011.

Priloga 3: Notranjost skimming naprave

Slika 5: Notranjost skimming napreve

Vir: Rear of ATM card skimming device captured by Perth police, 2012.

Priloga 4: Past za gotovino (angl. *cash trapping*)

Slika 6: Past za gotovino

Vir: Neue Betrugsmethode an Geldautomaten, 2011.

Priloga 5: Prikaz podatkov s pomočjo spletne aplikacije ter dopolnjeni podatki po obdelavi

Tabela 1: Prikaz podatkov s pomočjo spletne aplikacije ter dopolnjeni podatki po obdelavi

Naziv	**Titel**	**Vnos 1***	**Vnos 2…**
Dan prejete informacije	Date and Time recived information	23.1.2012	
Tip transakcije	Transaction Type	ATM	
Datum in čas transakcije	Date and Time, Local Transaction	21.1.2012; 18:21:33	
Datum in čas transakcije	Date and Time, Entry	18:21:33	
PAN	Masked Account Number	677014******	
TRR	Cardholder Account	**********	
Veljavnost	Date, Expiration	1409	
Oznaka prodajnega mesta	Card Acceptor Terminal Identification	BA01845N	
Lokacija	Card Accept or Name	ABA	
Lokacija	Card Acceptor Location	Spar	
Lokacija	Card Acceptor City	Slov. Bistrica	
Znesek v EUR	Amount, Cardholder Billing in EUR	50,00	
Način obveščanja	Way of information	Telefonsko	
Dan obveščanja	Date of information	23.1.2012	
Čas obveščanja	Time of information	10:15	
Opomba	Note		

Legenda: * primer vnosa

Vir: Banka X, Zlorabe plačilnih kartic in ukrepanje v OPP, 2012e, str. 6.