

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA ZAVAROVANJA ZLORAB PLAČILNIH KARTIC

Ljubljana, maj 2016

MARUŠA ČERV

IZJAVA O AVTORSTVU

Spodaj podpisana Maruša Červ, študentka Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtorica magistrskega dela z naslovom Analiza zavarovanja zlorab plačilnih kartic, pripravljenega v sodelovanju s svetovalcem izr. prof. dr. Alešem Berkom Skokom.

Izrecno izjavljam, da v skladu z določili Zakona o avtorskih in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) NE dovolim objave magistrskega 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
 - poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
 - pridobila 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 zapisala;
- 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 magistrskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne _____

Podpis avtorice: _____

KAZALO

UVOD	1
1 KARTIČNO POSLOVANJE V PLAČILNEM SISTEMU	3
1.1 Vrste plačilnih kartic	4
1.1.1 Plačilne kartice glede na izdajatelja	4
1.1.2 Plačilne kartice glede na način poravnave obveznosti	5
1.2 Razširjenost uporabe brezgotovinskega poslovanja in plačilnih kartic	6
1.2.1 Brezgotovinsko poslovanje v svetu	6
1.2.2 Brezgotovinsko poslovanje v Sloveniji	8
1.3 Delovanje sistema plačilnih kartic	9
1.4 Zgodovina plačilnih kartic	10
2 ZLORABE PLAČILNIH KARTIC	11
2.1 Oblike zlorab	13
2.1.1 Kraja identitete	14
2.1.2 Zlorabe izgubljenih ali ukradenih kartic	14
2.1.3 Zlorabe ponarejenih kartic	15
2.1.4 CNP-zlorabe	15
2.2 Kje se dogajajo zlorabe	15
2.2.1 Zlorabe kartic na internetu	15
2.2.2 Zlorabe na prodajnem mestu in na bančnem avtomatu	18
2.2.3 Zlorabe plačilnih kartic skozi zgodovino	20
2.3 Statistični podatki o zlorabah plačilnih kartic	21
2.3.1 Zlorabe plačilnih kartic v EU	21
2.3.2 Zlorabe plačilnih kartic v Sloveniji	22
2.3.3 Zlorabe plačilnih kartic v Angliji	23
3 VARNOST IN STANDARDI	24
3.1 Plačilne kartice po obdobjih	24
3.1.1 Magnetna kartica	25
3.1.2 Tehnologija po standardu EMV	25
3.1.3 Brezstična tehnologija	27
3.2 Skrb za varnost	28
3.2.1 PCI-standardi	28
3.2.2 Tokenizacija	31
3.2.3 Secure code	31
3.2.4 Ostali načini preprečevanja zlorab	32
4 ZAVAROVANJE ZLORAB PLAČILNIH KARTIC	34
4.1 Odgovornost pri zlorabah plačilnih kartic	35
4.1.1 Odgovornost na strani izdajatelja	35
4.1.2 Odgovornost na strani imetnika	35
4.1.3 Odgovornost za posamezno obliko zlorabe	36

4.1.4	Povračila za transakcije	37
4.2	Bančno zavarovalništvo	38
4.3	Razvoj zavarovalniških produktov	39
5	RAZISKOVALNI DEL	40
5.1	Prikaz možnosti zavarovanja plačilnih kartic v Sloveniji.....	40
5.2	Samostojni zavarovalni produkti zavarovalnic v Sloveniji	43
5.2.1	Zavarovalnica Triglav, d.d.....	43
5.2.2	Zavarovalnica Tilia, d.d.....	45
5.2.3	Zavarovalnica Maribor, d.d.	46
5.2.4	Primerjava samostojnih zavarovalnih produktov zavarovalnic v Sloveniji ..	48
5.3	Zavarovanje plačilnih kartic znotraj drugih produktov v sklopu kolektivnega zavarovanja imetnikov plačilnih kartic.....	50
5.3.1	Hypo Alpe-Adria-Bank, d.d.....	50
5.3.2	Raiffeisen banka, d.d.	51
5.3.3	Kartice Diners	51
5.4	Zavarovalni produkti v tujini	52
5.4.1	American Express za področje ZDA.....	52
5.4.2	Citibank Czech Republic, a.s.	53
5.4.3	Komerčni banka, a.s.	53
5.4.4	Sberbank CZ, a.s.	54
5.4.5	UniCredit Bank Czech Republic & Slovakia, a.s.	55
5.5	Pomanjkljivosti zavarovanja	56
5.6	Priložnosti za uvedbo novega produkta na trg.....	57
	SKLEP	59
	LITERATURA IN VIRI	61

KAZALO SLIK

Slika 1:	Naraščanje brezgotovinskega poslovanja v svetu.....	7
Slika 2:	Delež opravljenih transakcij s plačilnimi karticami najbolj znanih globalnih ponudnikov v letu 2013 v %.....	8
Slika 3:	Število izdanih plačilnih kartic v Sloveniji med letoma 2001 in 2015	9
Slika 4:	Zlorabe plačilnih kartic v EU in ZDA po obliki CNP in CP v %.....	13
Slika 5:	Prikaz oblik zlorab, ki zavzemajo največje deleže v EU med letoma 2009 in 2013 v %.....	22
Slika 6:	Podatki, ki so vidni na plačilni kartici	30
Slika 7:	Odgovornost za zlorabe plačilnih kartic po ZPlaSS	35
Slika 8:	Postopek reklamacije v primeru zlorabe plačilne kartice.....	38
Slika 9:	Možnosti, ki jih ima posameznik za sklepanje zavarovanja plačilnih kartic.....	41
Slika 10:	Primerjava zavarovalnih kritij za zavarovanje zlorabe plačilnih kartic pri slovenskih zavarovalnicah.....	49

KAZALO TABEL

Tabela 1:	Povprečna stopnja rasti brezgotovinskega poslovanja v svetu	6
Tabela 2:	Plačilne kartice in njihova uporaba v Sloveniji v letu 2014	8
Tabela 3:	Prikaz razvoja zlorab plačilnih kartic po obdobjih.....	21
Tabela 4:	Statistika kaznivega dejanja tatvine v primerih, ko je bil ukraden predmet tudi plačilna kartica med letoma 2011 in 2015	22
Tabela 5:	Statistika kaznivega dejanja uporabe ponarejenega plačilnega sredstva glede na način storitve med letoma 2011 in 2015	23
Tabela 6:	Statistika kaznivega dejanja goljufije v primerih, ko je bila plačilna kartica zlorabljena na internetu med letoma 2011 in 2015	23
Tabela 7:	Letna izguba zaradi zlorab v Angliji med letoma 2004 in 2014 (v milijonih funtov)	24
Tabela 8:	Načela PCI DSS	29
Tabela 9:	Varovani podatki po PCI DSS	30
Tabela 10:	Učinkovitost PCI DSS pri preprečevanju zlorab plačilnih kartic.....	30
Tabela 11:	Možnost zavarovanja zlorabe plačilne kartice posameznika po bankah oziroma hranilnicah v Sloveniji	41
Tabela 12:	Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Zavarovalnici Triglav, d.d.	44
Tabela 13:	Višina letne premije ob neposredni sklenitvi zavarovanja pri Zavarovalnici Triglav, d.d.....	45
Tabela 14:	Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Zavarovalnici Tilia, d.d.....	46
Tabela 15:	Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Zavarovalnici Maribor, d.d.	47

Tabela 16: Vrsta in višina zavarovalnih kritij za zavarovanje zlorabe kartic po posamičnih paketih HYPO Alpe Adria Bank, d.d.	50
Tabela 17: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Generali zavarovalnici, d.d. Ljubljana	51
Tabela 18: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Citibank CZ, a.s. (produkt: Fraudulent usage 50).....	53
Tabela 19: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Komerční banki, a.s. (produkt: Insurance against misuse of a card).....	53
Tabela 20: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Sberbank CZ, a.s. (produkt: Fraud Insurance for Payment Cards).....	54
Tabela 21: Obseg zavarovalnega kritja SAFE BASIC za zavarovanje zlorabe plačilnih kartic pri UniCredit Bank Czech Republic & Slovakia, a.s. (produkt: Insurance against card misuse).....	55
Tabela 22: Obseg zavarovalnega kritja SAFE PLUS za zavarovanje zlorabe plačilnih kartic pri UniCredit Bank Czech Republic & Slovakia, a.s. (produkt: Insurance against card misuse).....	56

UVOD

Poslovanja fizičnih in pravnih oseb brez plačilnih kartic si ne predstavljamo več, saj so postale nepogrešljive za takojšnje brezgotovinsko plačevanje, odložena plačila in obročno odplačevanje tako doma kot v tujini. Vsak imetnik transakcijskega računa pridobi bančno kartico BA Maestro, ki jo lahko uporablja za plačila na prodajnih mestih (angl. *point of sale*, v nadaljevanju POS) in za dvige na bankomatih (angl. *automatic teller machine* – ATM). Plačilne kartice imenujemo tudi »plastični denar«, saj se pojavljajo v standardizirani obliki plastičnih kartic (Lamberger, 2009, str. 29). Izjemno praktično uporabnost plačilnim karticam pripisujemo, ker omogočajo brezgotovinsko plačevanje, možnost dviga na bankomatu in enostaven nakup prek spleta. Nekatere plačilne kartice nam omogočajo nakup blaga in storitev celo v primeru, ko na računu nimamo dovolj sredstev. Govorimo o tako imenovanih karticah z odloženim plačilom in o nekaterih karticah zvestobe, ki nam jih ponujajo trgovci. Poleg udobja, hitrosti in drugih prednosti, ki jih prinaša brezgotovinsko poslovanje, pa smo ob uporabi izpostavljeni tudi številnim nevarnostim, saj tudi kriminalci gredo v korak s časom in sledijo tehnološkemu razvoju (Šavnik, 2008). Uporabo plačilnih kartic tako spremljajo zlorabe, prevare, goljufije in druga podobna dejanja. Zlorabe ne povzročajo stroškov samo potrošnikom, temveč vsem udeležencem v plačilnem procesu, tudi trgovcem in izdajateljem (Sullivan, 2008). Kljub temu, da izdajatelji plačilnih kartic zagotavljajo številne in vedno boljše varnostne ukrepe ter standarde, smo še vedno priča zlorabam (Voh Boštič, 2015). Če pride do zlorabe kartice, banke vsak primer obravnavajo individualno. Ko se ugotovi dejanski potek dogodkov, se tudi določi odgovornost banke in imetnika kartice. V primeru, da je za zlorabo odgovoren imetnik, bi k njegovemu občutku varnosti lahko prispevale tudi zavarovalnice s ponudbo ustreznega zavarovanja.

Glede na splošno nepoznavanje možnosti zavarovanja na področju plačilnih kartic podrobneje proučim, za katere vrste nevarnosti je možno zavarovati plačilne kartice, kaj nam na tem področju ponujajo domače in tuje zavarovalnice ter ali storitev ponujajo kot samostojen produkt ali v sklopu drugih zavarovanj. Potrošniki smo zaradi nenehnega razvoja priča vedno novim nevarnostim, zato se morajo tudi zavarovalnice prilagoditi in nam omogočiti varnost na področjih sodobne potrošnje (Vermeulen, 2004).

Namen magistrskega dela je na podlagi obstoječe literature raziskati in predstaviti zgodovino razvoja plačilnih kartic, vrste plačilnih kartic in statistično najpogostejše zlorabe, ki smo jim izpostavljeni imetniki plačilnih kartic. S proučitvijo ustrezne literature ugotovim, kako in v kolikšni meri smo imetniki sploh zaščiteni pred zlorabami (kakšni so varnostni ukrepi in standardi). Namen magistrskega dela je tudi opredeliti pomen razvoja sodobnih in potrošnikom prilagodljivih storitev v zavarovalništvu in predstaviti razvoj ter uvedbo nove storitve. Z magistrskim delom želim pridobiti koristne informacije, ki jih bom lahko uporabila za pripravo optimalne zasnove novega zavarovalnega produkta,

oblikovanega na podlagi kritične analize primerjalne presoje obstoječe ponudbe konkurentov.

Cilj magistrskega dela je predstaviti in primerjati zavarovanja plačilnih kartic, ki jih ponujajo izbrane zavarovalnice. Glavni cilj magistrskega dela je s primerjalno presojo ugotoviti, kaj za potrošnika predstavlja zanimiv in uporaben zavarovalni produkt na področju plačilnih kartic. S pridobljenimi rezultati bomo oblikovali sklep, kako naj bo nov produkt v zvezi z zavarovanjem plačilnih kartic zasnovan z vsebinskega vidika. Rezultati bi lahko služili kot podlaga za vpeljavo interne novosti v zavarovalnico.

Pri izdelavi magistrskega dela uporabim teoretično-analitična znanja, pridobljena s pomočjo relevantne domače in tuje literature. Magistrsko delo temelji tudi na pridobljenih notranjih virih izbranih in proučevanih zavarovalnic ter bank, ki ponujajo zavarovalne produkte za zavarovanje plačilnih kartic. S pomočjo primerjalne presoje na osnovi študije primera več zavarovalnic uporabim kombinacijo induktivnega in deduktivnega pristopa, da bi iz pridobljenih podatkov prišla do najboljše rešitve. Omejitve predstavljajo neenotno obravnavanje in razvrščanje oblik zlorab plačilnih kartic in posledično tudi neenotno vodenje evidenc o številu zlorab, zato sem za splošno opredelitev izbrala definicijo Europol. Zaradi poslovnih skrivnosti predstavlja dostop do podatkov o zlorabah, ki jih hranijo izdajatelji plačilnih kartic, dodatne omejitve, zato je bilo treba statistične podatke poiskati drugje. Naslednjo omejitev pripisujem iskanju predvsem tuje literature neposredno za zavarovanje plačilnih kartic, saj je ta zelo razpršena in jo pogosto tudi zaradi kompleksnosti področja ni mogoče izslediti. V nekaterih primerih je bila pridobitev ustreznih podatkov za analizo odvisna od pripravljenosti za sodelovanje zaposlenih v določenem podjetju. Pri nekaterih izdajateljih oziroma zavarovalnicah mi tako ni uspelo pridobiti vseh podatkov, ki bi izboljšali analizo, na spletu pa tudi niso dostopni, zato so bili iz analize po večini izključeni.

Struktura dela. Magistrsko delo je razdeljeno na pet poglavij. V prvem poglavju opredelim kartično poslovanje v plačilnem sistemu, vrste plačilnih kartic in trende v brezgotovinskem poslovanju. Predstavim tudi sistem delovanja plačilnih kartic in zgodovino njihovega razvoja. Sledi drugo poglavje, kjer predstavim oblike zlorab plačilnih kartic, kje vse se lahko zlorabe zgodijo in statistične podatke o zlorabah plačilnih kartic. V tretjem poglavju opišem izboljšani razvoj varnosti plačilnih kartic ter varnostne mehanizme in standarde, ki jih na področju kartičnega poslovanja zagotavljajo izdajatelji. Četrto poglavje je namenjeno ponazoritvi odgovornosti vpletenih pri posamezni obliki zlorabe. V nadaljevanju poglavja predstavim, od kje sploh izvira potreba posameznika po zavarovanju, prav tako pa, zakaj banke ponujajo produkte zavarovalnic. Na koncu poglavja sledi še predstavitev razvoja zavarovalnih produktov. V petem poglavju magistrskega dela preidem na raziskovalni del, kjer natančneje analiziram možnosti zavarovanja plačilnih kartic v Sloveniji in tujini. V nadaljevanju poglavja sledijo primerjava in predlogi za obogatitev ponudbe zavarovalnih produktov za zavarovanje plačilnih kartic v Sloveniji.

1 KARTIČNO POSLOVANJE V PLAČILNEM SISTEMU

Za potrebno razumevanje kartičnega poslovanja so v nadaljevanju opredeljeni trije glavni pojmi v bančništvu, ki jih povezujemo s plačilnimi karticami, in sicer plačilni sistem, plačilni promet in plačilni instrumenti.

Plačilni sistem v državi določa postopke, pravila, standarde in instrumente, ki se uporabljajo pri izmenjavi finančnih sredstev med dvema strankama ob poravnavi njunih dolžniško-upniških razmerij (Slabe Cepec & Lekše, 2009). Plačilni sistem spodbuja ekonomske aktivnosti, zmanjšuje stroške transakcij in omogoča razvoj finančnega sektorja z razvojem novih storitev ter z varnostjo. Plačilni sistem zagotavlja varne, učinkovite in pravočasne poravnave finančnih transakcij ter tako prispeva k tekočemu delovanju finančnih trgov in s tem k splošni stabilnosti in učinkovitosti gospodarstva (Koma, 2001; Plačilni in poravnalni sistemi, 2016). Pomembnost plačilnega sistema se kaže tudi v zmožnosti tekočega izvajanja plačilnih transakcij ter zaupanju uporabnikov v varnost in učinkovitost izvajanja transakcij (Kovač, 2011, str. 53).

Plačilni promet predstavljajo vsa plačila, opravljena med fizičnimi in pravnimi osebami. Pomeni torej kroženja denarja. Potekati mora urejeno, po nekem sistemu in določenih pravilih, kar ureja plačilni sistem države. Udeleženci v plačilnem prometu so: poslovne ali komercialne banke, centralna banka, medbančni operacijski center in komitenti bank, tako podjetja kot državljani (Slabe Cepec & Lekše, 2009). Banka se tako v procesu pojavi kot tretja oseba, prek katere se opravljajo plačila med fizičnimi in pravnimi subjekti. Denar v gotovinski obliki se v plačilnem prometu pojavlja kot plačilno sredstvo, medtem ko potrebuje brezgotovinski plačilni promet posebne plačilne instrumente. Glede na sedež oseb, udeleženih v plačilnem prometu, ločimo notranji in zunanji mednarodni plačilni promet. V primeru, da ima ena od oseb, ki so udeležene v procesu, sedež v tujini, pa govorimo o mednarodnem plačilnem prometu (Lamberger, 2011, str. 12).

Plačilni instrumenti so različne oblike plačevanja (plačilne kartice, plačilne nalogi). V najširšem pomenu so plačilni instrumenti vsa sredstva, ki imetniku omogočajo brezgotovinski prenos sredstev oziroma dvig gotovine (Plačilni instrumenti, 2016). Plačilni instrument je vsaka naprava ali niz postopkov (oziroma oboje), ki so dogovorjeni med posameznim uporabnikom in njegovim ponudnikom plačilnih storitev, in je vezan le na tega uporabnika z namenom, da ga uporabi za odreditev naloga za poravnavo (Zakon o plačilnih storitvah in sistemih, Uradni list RS št. 58/09, 34/10, 9/11, 32/12 in 81/15) – (v nadaljevanju ZPlaSS).

1.1 Vrste plačilnih kartic

V sodobnem svetu smo priča množični uporabi brezgotovinskega poslovanja, ki nam ga omogočajo plačilne kartice, prav tako sta vedno bolj priljubljena nakupovanje prek spleta in elektronsko bančništvo. S plačilnimi karticami smo obkroženi praktično na vsakem koraku, doživljamo jih že kot samoumevne. Prav tako so v izjemnem porastu tudi različne kartice podjetij, ki tudi omogočajo plačilo brez gotovine. Glavni namen plačilnih kartic je potrošniku nuditi udobnejše, enostavnejše in priročnejše poslovanje. S plačilnimi karticami je vsak dan na vseh koncih sveta opravljenih na milijone transakcij. Ljudje z njimi plačujemo prehrano, obleke, čevlje, darila, knjige, rezerviramo letalo oziroma hotel, plačamo za gorivo, jemo v restavraciji itd. (Slawsky & Zafar, 2005, str. 1).

Lamberger, Dobovšek in Slak (2012) pravijo, da so plačilne kartice plačilni instrument, ki ima za razliko od gotovine večjo uporabnost, saj lahko z njimi plačujemo izdelke in storitve neodvisno od valute ter tudi na daljavo, pri uporabi kreditnih kartic pa tudi brez trenutno razpoložljivih finančnih sredstev. Razvrščamo jih po različnih kriterijih, s pravnega in finančnega vidika pa sta pomembna predvsem kriterij izdajatelja plačilne kartice in načina poravnave obveznosti (Plačilni instrumenti, 2016).

1.1.1 Plačilne kartice glede na izdajatelja

Po kriteriju izdajatelja delimo plačilne kartice na bančne in nebančne. Bančne so tiste, ki jih izdajajo banke in hranilnice, nebančne pa so plačilne kartice večjih trgovskih podjetij in plačilne kartice družb, katerih izključna dejavnost je izdajanje kreditnih plačilnih kartic (Plačilni instrumenti, 2016).

Domače in licenčne plačilne kartice. Banke in hranilnice izdajajo različne vrste plačilnih ter kreditnih kartic, in sicer samostojno ali na podlagi sklenjene licenčne pogodbe s tujim partnerjem (licenčne). Domače plačilne kartice (Activa, Karanta) so tiste, ki se uporabljajo za plačila izključno v slovenskem prostoru. Licenčne plačilne kartice pa je mogoče uporabljati za plačila v Sloveniji in tujini. Izdajatelji licenčnih kartic s sklenitvijo pogodbe z licenčnim partnerjem pristanejo na pravila poslovanja, ki veljajo za celotno poslovanje s karticami določene blagovne znamke (Šteblaj, 1999).

Bančne in podjetniške kartice. Bančne plačilne kartice so vse plačilne kartice, ki jih izdajajo banke samostojno oziroma na podlagi sklenjene licenčne pogodbe. Podjetniške plačilne kartice pa izdajajo podjetja za svojo trgovsko verigo samostojno (Mercator Pika, Petrol klub plačilna kartica zvestobe itd.) ali pa na podlagi sklenjene licenčne pogodbe z mednarodnimi izdajatelji.

Izdajatelji lahko izdajo kartice fizičnim (osebne kartice) in pravnim osebam (poslovne kartice). Slednje so namenjene vodilnim in drugim delavcem v podjetju za plačilo potovalnih, reprezentančnih in drugih stroškov ali nakupov (Šteblaj, 1999).

1.1.2 Plačilne kartice glede na način poravnave obveznosti

Glede na način poravnave obveznosti ločujemo med debetnimi in kreditnimi plačilnimi karticami. Debetna plačilna kartica imetniku omogoča opravljanje plačil tako, da izdajatelj kartice ob vsaki uporabi takoj obremeni njegov transakcijski račun za znesek opravljenih plačil, kreditna plačilna kartica pa imetniku odobri posojilo oziroma odlog plačila in omogoča nakupe ali dvige gotovine do vnaprej dogovorjene zgornje meje odobrenega posojila (Plačilni instrumenti, 2016).

Poznamo štiri različne tipe plačilnih kartic (OECD, 2002):

- kartice s kasnejšim plačilom (kreditne kartice in kartice z odlogom plačila),
- kartice s takojšnjim plačilom (debetne kartice) in
- predplačniške kartice.

Debetne kartice (angl. *pay now cards*). Debetna kartica nam omogoča opravljanje plačil in dvig gotovine iz razpoložljivih sredstev na računu, uporablja pa se tako za nakupe na prodajnih mestih kakor za dvig gotovine z bančnega avtomata (Maestro kartica, 2016). Za debetne kartice je značilno, da se ob nakupu blaga/plačila storitve stanje na našem računu takoj zmanjša za vrednost nakupa (Maurer, 2009). Mann (v Robertson, 2014, str. 507–508) pravi, da je glavna funkcija debetnih kartic omogočanje uporabniku, da se s plačilom prek plačilnega terminala izvrši prenos sredstev z bančnega računa do trgovca. Plačilni terminal preveri pristnost kartice in ugotovi, ali je na uporabnikovem računu dovolj sredstev. V primeru, da izdajatelj kartice odobri transakcijo, se sredstva prenesejo z uporabnikovega računa na trgovčevega. Debetne plačilne kartice pomagajo potrošnikom upravljati z njihovimi sredstvi, finančna institucija pa preprečuje prekoračitev limita transakcije na prodajnem mestu (Lamb, 2001). V Sloveniji so se debetne kartice prvič pojavile v letu 1997, ko so postopno začele izpodrivati dotedanje čekovne kartice in imetnikom kot prve omogočale tudi debetno poslovanje na elektronsko opremljenih prodajnih mestih (POS-terminal) (Šteblaj, 1999).

Kreditne kartice (angl. *pay letter cards*). Klasična kreditna kartica imetniku omogoča »izposojlo« finančnih sredstev za dvig gotovine oziroma plačilo blaga in storitev. Uporabniku je tako odobreno okvirno posojilo v določeni višini, ki je odvisno od mesečnih prilivov. Uporabnik mora izposojeni znesek vrniti v dogovorjenih mesečnih obrokih. Del obveznosti se tako plača v tekočem mesecu, preostanek pa se prenese v naslednji mesec. Pri drugi vrsti kreditne kartice pa gre pravzaprav za kreditne kartice z odloženim plačilom (angl. *revolving*), pri katerih je izdajatelju kartice treba poravnati transakcije, opravljene s

to kartico, po navadi enkrat mesečno na določen dan. Slednja vrsta kreditnih kartic je večinoma prisotna v Evropi, medtem ko v ZDA bolj uporabljajo klasične kreditne kartice (Maurer, 2009).

Kot ugotavlja Odar (2010), je plačilo s kreditno kartico enako plačilu z izposojenim denarjem. Uporabnikom kreditnih kartic je najpomembnejša njihova značilnost kreditiranja, saj lahko kupujejo blago ali storitve tudi v primeru, če trenutno nimajo razpoložljivih sredstev na računu. Največji prednosti sta torej kreditiranje in preprosto brezgotovinsko poslovanje. Izdajateljem kreditnih kartic pa je največja prednost, da od izdaje kreditne kartice poberejo članarino, omogočajo pa le kratko kreditiranje, zato dobijo svoja sredstva v določenem kratkem časovnem obdobju povrnjena. Največja prednost za prodajalce pa je, da kupci kupijo blago ali storitve tudi v primeru, če na računu nimajo dovolj sredstev, oziroma si privoščijo tudi dražje dobrine, ki si jih sicer ne bi, izdajatelj kreditne kartice pa jim jamči za plačilo, opravljeno s kreditno kartico.

Predplačniške kartice (angl. *pay before cards*). Predplačniške kartice so vse pogostejši del bančne ponudbe, za večino potrošnikov pa so še novost. Predplačniška kartica je plačilna kartica, na katero je možno naložiti denar ter jo uporabljati za nakupe na prodajnih mestih, dvig gotovine na bančnem avtomatu ter za spletne nakupe. Dobroimetje na kartici ni vezano na bančni račun, porabiti je možno le toliko, kolikor je na kartici naloženega. Bančni račun ni potreben za izdajo predplačniške kartice, saj je povezana s posebnim računom, kjer se hrani naloženi denar (Krisper & Meško, 2015).

1.2 Razširjenost uporabe brezgotovinskega poslovanja in plačilnih kartic

1.2.1 Brezgotovinsko poslovanje v svetu

Tabela 1 prikazuje povprečno stopnjo rasti brezgotovinskega poslovanja po različnih predelih sveta.

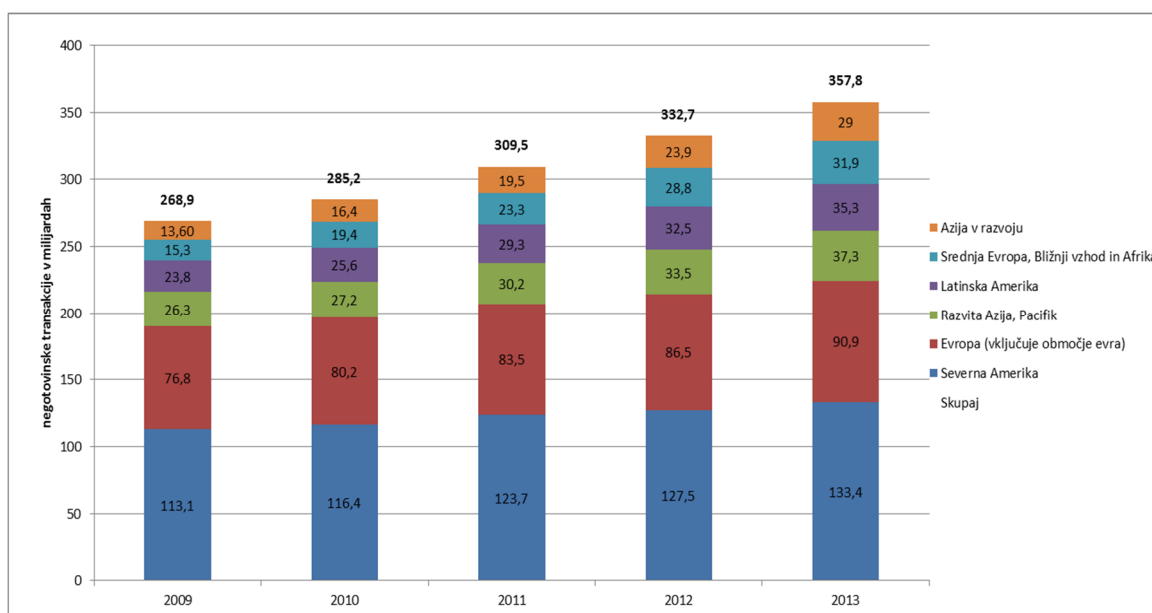
Tabela 1: Povprečna stopnja rasti brezgotovinskega poslovanja v svetu

Območje	Globalno	Azija v razvoju	Srednja Evropa, Bližnji vzhod in Afrika	Latinska Amerika	Razvita Azija, Pacifik	Evropa (vključuje območje evra)	Severna Amerika
Stopnja rasti v letu 2013 glede na 2009 v %	7,4	20,9	20,1	10,4	9,1	4,3	4,2

Vir: Capgemini, Number of Worldwide Non-Cash Transactions for North America, Europe, Mature APAC, Latin America, CEMEA and Emerging Asia in 2009, 2010, 2011, 2012, 2013 and 2014E, (b.l.).

Kot opazimo iz Tabele 1, najvišjo stopnjo rasti pri uporabi brezgotovinskega poslovanja beležijo azijske države v razvoju, kjer je ta v letu 2013 glede na leto 2009 znašala 20,9 %. Najnižjo stopnjo rasti so zaradi dolgoletne uporabe brezgotovinskega poslovanja zaznali v Severni Ameriki, kjer je znašala 4,2 %, stopnja rasti na globalni ravni pa je znašala 7,4 %. Slika 1 prikazuje, kako brezgotovinsko poslovanje v zadnjih letih narašča.

Slika 1: Naraščanje brezgotovinskega poslovanja v svetu



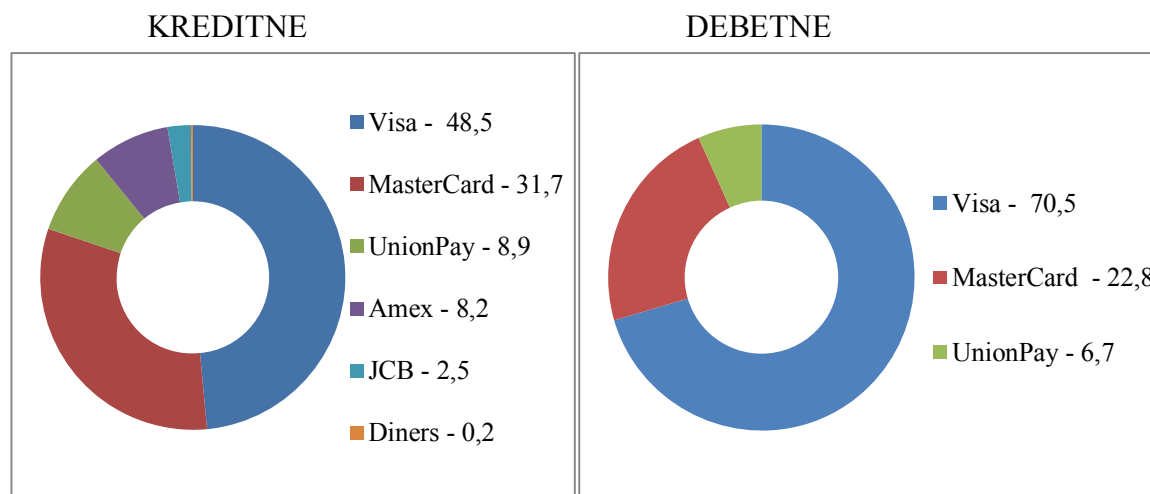
Vir: Capgemini, Number of Worldwide Non-Cash Transactions for North America, Europe, Mature APAC, Latin America, CEMEA and Emerging Asia in 2009, 2010, 2011, 2012, 2013 and 2014E, (b.l).

Iz Slike 1 je razvidno, da je svetovno prebivalstvo v letu 2013 opravilo za skoraj 360 milijard brezgotovinskih transakcij. Največji delež brezgotovinskih transakcij je bil opravljen v Severni Ameriki in Evropi, najmanjši pa v azijskih državah v razvoju.

Skupno število brezgotovinskih plačil je v letu 2014 v Evropski uniji (v nadaljevanju EU) naraslo za 2,8 % glede na leto 2013. Brezgotovinska plačila tako predstavljajo 46 % vseh opravljenih transakcij v EU (Payment Statistics for 2014, 2015).

Slika 2 prikazuje deleže opravljenih transakcij s kreditnimi in debetnimi karticami najbolj znanih ponudnikov plačilnih kartic, ki so: Visa, MasterCard, UnionPay, Amex, JCB in Diners (The Nilson Report, 2015).

Slika 2: Delež opravljenih transakcij s plačilnimi karticami najbolj znanih globalnih ponudnikov v letu 2013 v %



Vir: The Nilson Report, Purchase Transactions On Global Cards 2013, 2015.

1.2.2 Brezgotovinsko poslovanje v Sloveniji

V Tabeli 2 predstavljam število izdanih plačilnih kartic v Sloveniji, obseg opravljenih plačil z njimi ter njihovo vrednost.

Tabela 2: Plačilne kartice in njihova uporaba v Sloveniji v letu 2014

Vrsta plačilnih kartic	Št. izdanih plačilnih kartic v Sloveniji	Št. plačil v Sloveniji (v tisoč)	Vrednost plačil (v mio EUR)
Kreditne kartice	1.855.561	58.669	2.289
Domače	1.164.287	26.248	1.047
Tuje	691.274	32.421	1.242
Bančne	714.028	35.168	1.191
Podjetniške	1.141.533	23.501	1.098
Osebne	1.604.353	53.221	1.593
Poslovne	251.208	5.448	696
Debetne kartice	2.404.544	91.467	2.917

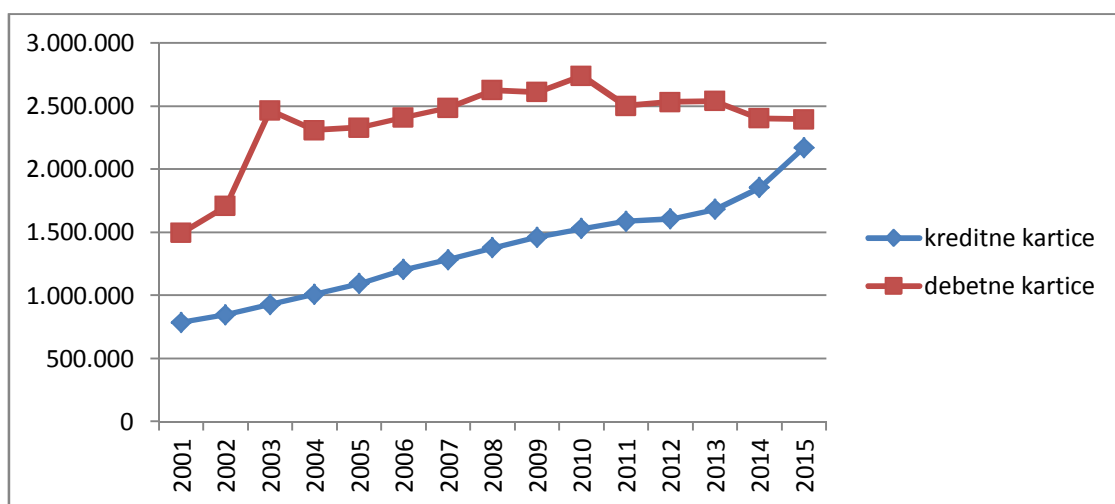
Vir: Banka Slovenije, Bilten Banke Slovenije, 2015, str. 43.

Po podatkih Banke Slovenije je bilo na dan 31. 12. 2014 v uporabi skupaj več kot 2,4 milijona debetnih in 1,8 milijona kreditnih kartic. Tako po številu plačil kot po vrednosti plačil prednjačijo debetne kartice. Glavni razlog za to se najbrž skriva v dejstvu, da ob odprtju osebnega računa na banki vsak uporabnik prejme debetno kartico. Iz podatkov za leto 2014 opazimo, da fizične osebe opravijo glavnino prometa s kreditnimi karticami. Kot je razvidno iz Tabele 2, je bilo leta 2014 več domačih plačilnih kartic kot licenčnih, kljub

temu pa je bila z licenčnimi karticami ustvarjena višja vrednost plačil. V primerjavi bančnih in podjetniških kartic opazimo, da je bilo izdanih več slednjih, vendar je bila pri teh vrednost plačil nekoliko nižja. Poslovnih kartic, ki jih banke izdajo podjetjem, je bilo v primerjavi s karticami, izdanimi fizičnim osebam, zelo malo. Poslovne kartice so ustvarile le dobro četrtino vrednosti plačil v primerjavi z osebnimi karticami.

Slika 3 nazorno prikazuje gibanje števila izdanih kartic v zadnjih 15 letih v Sloveniji.

Slika 3: Število izdanih plačilnih kartic v Sloveniji med letoma 2001 in 2015



Vir: Banka Slovenije, Bilten Banke Slovenije, 2016, str. 43.

Iz Slike 3 je razvidno naraščanje števila izdanih plačilnih kartic med letoma 2001 in 2015 v Sloveniji. Število izdanih kreditnih kartic se vsako leto nekoliko poveša, pri številu izdanih debetnih kartic pa v zadnjih letih opazimo manjši upad.

1.3 Delovanje sistema plačilnih kartic

Plačilne transakcije s plačilnimi karticami večinoma potekajo po štiristranski kartični shemi. Vsak udeleženec ima ključno vlogo pri oblikovanju plačilne transakcije, skupaj pa zagotavljajo, da so sprejete transakcije varne in učinkovite; kartična shema pa omogoča platformo za izmenjavo transakcij. Ključni udeleženci štiristranske kartične sheme so (OECD, 2002; Slawsky et al., 2005, str. 12):

- **imetnik kartice** (angl. *the cardholder*) – oseba, ki ji izdajatelj plačilnih kartic izda kartico za dvig gotovine ter opravljanje nakupov;
- **izdajatelj** (angl. *the issuer*) – finančna institucija ali drugo podjetje, ki imetniku zagotavlja kartico in račun;
- **prodajno mesto** (angl. *the merchant*) – vsako prodajno mesto ali storitvena dejavnost, ki izpolnjuje pogoje za sprejem plačilnih kartic. Ima poslovno razmerje s pridobiteljem;

- **pridobitelj** (angl. the *acquirer*) – v literaturi je včasih omenjen kot banka trgovca, je finančna ustanova, ki prodajnim mestom omogoča, da izpolnjujejo procesne obveznosti pri sprejemanju plačil.

Vse transakcije ne glede na to, kako so opravljene, morajo biti nekje obdelane. Vlogo obdelovanja kartičnih plačil po navadi prevzemajo procesni centri, to so poslovni subjekti, s katerimi ima banka sklenjeno pogodbo za obdelavo in prenos podatkov pri transakciji s kartico. V Sloveniji delujejo naslednji centri za procesiranje kartic (Kartice, 2016):

- Bankart, d.o.o., izvaja procesiranje Karante ter mednarodnih kartičnih shem Maestro, MasterCard in Visa ter procesiranje bankomatskega prometa v Sloveniji za 16 domačih ponudnikov plačilnih storitev;
- IntesaSanPaoloCard, d.o.o., izvaja procesiranje blagovne znamke Activa ter mednarodnih kartičnih shem MasterCard in Visa za osem domačih ponudnikov plačilnih storitev;
- eFunds International Limited, Podružnica v Ljubljani, procesira kartice MasterCard in Visa za enega domačega ponudnika plačilnih storitev.

1.4 Zgodovina plačilnih kartic

Prve plačilne kartice so se pojavile v začetku dvajsetega stoletja v Združenih državah Amerike (v nadaljevanju ZDA). Za njihovo uporabo so kot prve zaslužne velike naftne družbe, ki so kupcem na svojih prodajnih mestih omogočale prvo brezgotovinsko poslovanje (Slawsky et al., 2005, str. 2). Nadalje so se jim pridružile verige hotelov in velikih trgovin, ki so kartice začele izdajati svojim večjim potrošnikom (Woolsey & Gerson, 2009). Proti sredini dvajsetega stoletja so banke pričele iskati način, kako bi se uspešno uveljavile s ponudbo plačilnih kartic, a pri tem niso bile dovolj hitre (Slawsky et al., 2005, str. 2). Najpomembnejši korak v zgodovini plačilnih kartic sega v leto 1949, ko je ameriški poslovnež Frank McNamara v neko restavracijo na večerjo povabil svoje poslovne partnerje. Ugotovil je, da s seboj nima gotovine, da bi poravnal račun. McNamara se je nato domislil, zakaj smo ljudje za plačilo blaga ali storitev omejeni le z gotovino, ki jo imamo pri sebi, namesto da bi lahko zapravili toliko, kolikor si lahko privoščimo. Tako je nastala prva ideja o uvedbi brezgotovinskega poslovanja. Leto kasneje se je gospod s poslovnim partnerjem ponovno znašel v isti restavraciji. Ko je natakar prinesel račun, se je Frank McNamara predstavil z manjšo kartonasto kartico – Diners Club Card – in se podpisal na račun. Beseda Diners izhaja iz angleške besede *dinner* in v slovenščini pomeni večerja, zato je dogodek v zgodovini kreditnih kartic znan kot »prva večerja«. S prvo izdano plačilno kartico je bilo sprva mogoče plačevati le prehrano v štirinajstih restavracijah v New Yorku (Woolsey et al., 2009). Brezgotovinsko plačevanje se je hitro razširilo med potrošniki in trgovci, saj so lahko boljše izkoristili kupno moč svojih strank. Ideja brezgotovinskega plačevanja je kmalu tudi presegla meje ZDA, saj je Diners Club

leta 1952 pričel izdajati prve mednarodne kartice (Zgodovina pametnih kartic, 2015). Proti koncu leta 1950 je tudi Bank of America izdala svojo prvo plačilno kartico. Hitro si je pridobila zaupanje potrošnikov, zato je število izdanih plačilnih kartic znatno naraslo do leta 1960, ko je bila izdana že milijonta kartica, od tedaj pa je njihovo število le še v vzponu. V tem času se je Bank of America uspešno razvijala in se preimenovala v BankAmericard. Na podlagi licenčne pogodbe so drugim bankam ponudili uporabo svojih plačilnih kartic, saj te niso imele dovolj sredstev za razvoj svojega produkta. To pomeni tudi prelomen trenutek v razvoju plačilnih kartic. Uspeh BankAmericarda je pripomogel k vzpostavitvi konkurence na tem področju in tako je bilo leta 1966 ustanovljeno kartično združenje The Interbank Card Association. Zaradi boljše prepoznavnosti in razvoja močnejše blagovne znamke se je združenje leta 1969 preimenovalo v »Master Charge«, leta 1979 pa v »MasterCard«, kar poznamo še danes. Začetki Vise segajo v leto 1974, ko je Bank of America razširila svoje poslovanje preko meja ZDA in ustanovila podjetje IBANCO, ki se je leta 1976 preimenovalo v Visa International (Zgodovina pametnih kartic, 2015; Slawsky et al., 2005).

Po navedbah (Slawsky et al., 2005) se plačilne kartice niso razvile samo zato, ker ljudje niso imeli dovolj sredstev za plačilo, temveč tudi zato, ker niso želeli prenašati kupov gotovine s seboj ves čas in ker je plačevanje s plačilnimi karticami udobnejše ter načeloma varnejše.

Plačilne kartice so za potrošnike postale še bolj privlačne v začetku 80. let z razvojem bančnih avtomatov (Carbó Valverde & Rodríguez Fernández, 2014). Elektronska tehnologija za plačilo na prodajnem mestu se je razvila leta 1979, ko je družba Visa predstavila prvi elektronski plačilni terminal (Evans & Schmalensee, 2009). Še v 90. letih si niti v ZDA nihče ni predstavljal manjših nakupov, ki bi jih lahko poravnal s plačilno kartico. Ta navada se je bistveno spremenila v letu 2003, ko so plačila s plačilnimi karticami že predstavljala več kot polovico plačil (Kjos, 2007).

Prva plačilna kartica v Sloveniji je bila American Express, ki smo jo pričeli uporabljati leta 1968, kasneje pa so se ji pridružile še druge licenčne kartice kakor tudi domače kartice (Plačilne kartice, 2016). Visa, MasterCard in American Express so danes globalno prepoznane znamke, ki procesirajo potrošniška in poslovna plačila na globalni ravni. Njihova uspešnost ni samo potrošnikom ponuditi udobnejši način za plačilo, temveč tudi prodajalcem omogočati prodajo brez tveganja (Slawsky et al., 2005).

2 ZLORABE PLAČILNIH KARTIC

Razširjenost uporabe plačilnih kartic je pripeljala do tega, da smo na tovrsten plačilni instrument postali izjemno navezani. Plačilne kartice uporabnikom omogočajo udobno in hitro trošenje sredstev na računu, goljufo pa razširjenost uporabe po vsem svetu ponuja vedno nove priložnosti za kazniva dejanja. Tako kot je v svetu priljubljeno plačevanje s

plačilnimi karticami, se je treba zavedati tudi številnih oblik zlorab, ki nas ogrožajo. Ustrezna varnost poslovanja s plačilnimi karticami je ključnega pomena, saj se storilci znajo še prehitro prilagoditi varnostnim novostim in tehnološkemu napredku.

Po statističnih ocenah je samo v ZDA že 10 % imetnikov plačilnih kartic postalo žrtev zlorabe (Credit Card Fraud Statistic, 2015). Goljufije predstavljajo grožnjo učinkovitosti plačilnega sistema, saj degradirajo učinkovitost in povzročajo stroške vsem udeležencem v plačilnem sistemu, tako trgovcem, imetnikom kot izdajateljem. Poleg tega povzročajo tudi posredne stroške nacionalnim organom pregona, postavljajo ovire za spletne trgovine in splošne ovire za sprejem elektronskih plačil (Sullivan, 2008).

Zlorabe plačilnih kartic lahko v grobem opredelimo kot katerokoli dejavnost, kjer se uporablja zaupne osebne ter finančne informacije za pridobitev protipravnih premoženjskih koristi (Cheney, Hunt, Jacob, Porter, & Summers 2012).

Zloraba plačilnih kartic je ena izmed večjih groženj današnjim poslovnim procesom. Za boj proti temu je najprej treba sploh razumeti oblike goljufije (Bhatla, Prabhu, & Dua, 2003). Zloraba plačilnih kartic se lahko zgodi v kateremkoli delu procesa njihove uporabe, celo ob izdaji, ko si kriminalci s krajo identitete pridobijo plačilno kartico s podatki tretjih oseb (Lamberger et al., 2012).

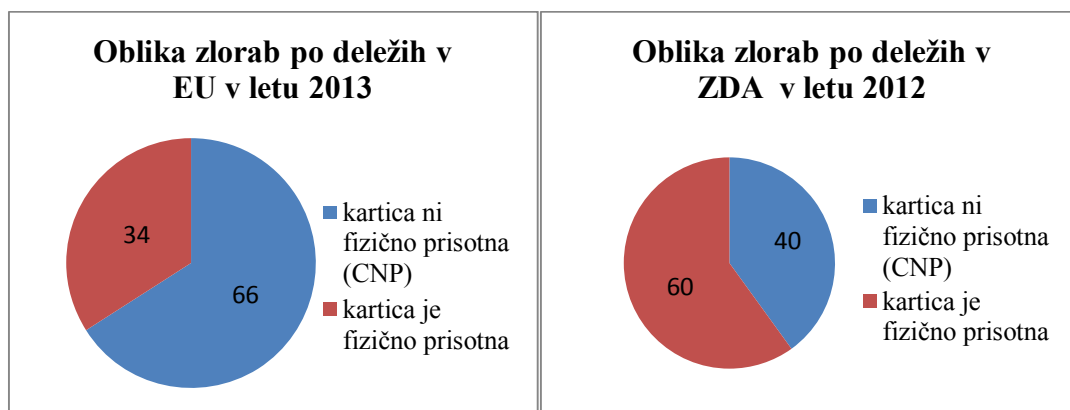
Zlorabe plačilnih kartic predstavljajo donosen posel za organizirane kriminalne združbe, ki razvijajo in izkoriščajo vse mogoče oblike te vrste kaznivega dejanja. Pogosto so značilne povezave med kriminalci in finančnimi ustanovami, dobro poznavanje tehnoloških novosti in varnostnih mehanizmov (Zupančič, 1999).

Souvignet, Hatin, Maqua, Tesniere, Leger in Hormiere zlorabe plačilnih kartic (2014, str. 144) delijo na:

- **kartica ni fizično prisotna** (angl. *card not present*, v nadaljevanju CNP);
- **kartica je fizično prisotna** (angl. *card present*, v nadaljevanju CP). Tovrstna zloraba se v grobem nanaša na pridobljene podatke iz ukradenih ali izgubljenih kartic, skimming, shimming ter preostale mogoče zlorabe bančnih avtomatov.

Razlike v razmerju med CNP- in CP-zlorabami v ZDA in EU prikazuje Slika 4.

Slika 4: Zlorabe plačilnih kartic v EU in ZDA po obliki CNP in CP v %



Vir: European Central Bank, *Fourth report on card fraud*, 2015, str. 11, tabela A.

Po podatkih Evropske centralne banke (v nadaljevanju ECB) je bila v letu 2013 v EU najpogostejša oblika goljufije plačilnih kartic oblika CNP, saj predstavlja kar 66 % vseh zlorab. Oblika goljufije, kjer je za zlorabo potrebna fizična prisotnost kartice (CP), pa je predstavljala preostalih 34 % vseh zlorab. V EU je tudi v prihodnje za pričakovati več CNP-zlorab, predvsem zaradi migracije goljufov iz CP, kjer je zloraba zaradi integracije EMV postala bistveno težja. Prav nezadostna integracija standarda EMV pa je tudi razlog, da so leta 2012 v ZDA še vedno večino zlorab (60 %) predstavljale CP-goljufije (Payments cards and mobile, 2015, str. 5).

2.1 Oblike zlorab

Zlorabe se dogajajo v fizičnem in kibernetskem prostoru. Glede na široko uporabo tehnologije (računalniki, mobilne naprave in internet) smo ljudje v kibernetskem prostoru povezani praktično na vsakem koraku, ta povezanost pa nudi priložnosti tudi kibernetski kriminaliteti, povezani z računalniki. Ker je tehnologija dostopna vsakomur in za njeno uporabo ne potrebujemo pretiranega znanja, uporabniki tudi dejansko ne razumejo, katere grožnje v kibernetskem prostoru pretijo, zato pogosto poteka uporaba brez ustrezne zaščite. Ustrezna zaščita je torej odvisna tudi od ustreznega in odgovornega obnašanja v kibernetskem prostoru (Bernik & Prislan, 2012, str. 30, 31).

Po podatkih Interpola so najpogostejše vrste goljufij s plačilnimi karticami (Payment cards, 2016):

- kraja identitete – lažna vloga/prevzem računa tretje osebe,
- zlorabe izgubljenih ali ukradenih kartic,
- zlorabe s ponarejenimi karticami,
- CNP-zlorabe, in

- zlorabe na bančnih avtomatih.

2.1.1 Kraja identitete

Kraja identitete v povezavi s plačilnimi karticami se najpogosteje zgodi na dva načina: uporaba osebnih podatkov za odprtje novega računa – **lažna vloga** ali pa uporaba osebnih podatkov za zlorabo obstoječega računa – **prevzem računa** (Payment cards, 2016).

Lažna vloga (angl. *application fraud*) se zgodi, ko storilec pridobi podatke žrtve iz ukradenih ali ponarejenih dokumentov ter odpre račun v imenu nekoga drugega (Payment cards, 2016). Po navedbah Bhatla et al. (2003) pa lažna vloga pomeni tudi finančno goljufijo, kjer posameznik navede napačne podatke o svojem finančnem stanju za pridobitev posojila. Najpogostejša vrsta – kraje identitete je zloraba obstoječega računa (angl. *account takeover*) in računov spletnih plačil (na primer PayPal). Gre predvsem za prevaro izdajatelja kartice za ponovno izdajo kartice ter preusmeritev te na drug naslov (Završnik, 2015, str. 47; Payment cards, 2016).

V literaturi zasledimo še druge klasifikacije kraje identitete. Vsem je skupno, da kriminallec kaznivo pridobi osebne podatke posameznikov in tako prevzame identiteto žrtve ter upravlja z njenim računom oziroma odpira nove račune (Sullivan, 2008). Goljufi pridobijo podatke za krajo identitete na različne načine. Bančni izpiski vsebujejo zaupne podatke, kot so ime, naslov in številka kartice, in če ti niso ustrezno uničeni, lahko imetnik postane žrtev. V kibernetnem prostoru pa je podatke mogoče pridobiti: z lažnim predstavljanjem, zvabljanjem, škodljivo programsko opremo ali vdorom v informacijski sistem z velikimi podatkovnimi zbirkami. Kriminallec tako lahko z uporabo zaupnih podatkov aktivira nov kreditni račun brez vednosti imetnika (Brody, Brown, Chettry, & White, 2014; Završnik, 2015, str. 47).

2.1.2 Zlorabe izgubljenih ali ukradenih kartic

Pridobitev izgubljenih ali ukradenih kartic je najbolj tradicionalna oblika, ki vodi v zlorabo kartic. Ta praksa se sicer nekoliko zmanjšuje zaradi uporabe učinkovitih protiukrepov, za kar je zaslužna predvsem uporaba kartic s standardom EMV (več v nadaljevanju) (Pavia, Vernes-Ferrer, & Foix-Escura, 2012). Obstaja več načinov, kako tatovi pridejo do kartic. Prvi način je neposredna kraja, kjer je kartica glavni motiv roba. V drugem primeru pa storilci pridejo do kartic v primeru vloma/ropa, kjer je kartica v posrednem planu. Sicer pa lahko kartico tudi izgubimo. Kriminallec, ki pridobi tujo plačilno kartico, ne glede na to, ali je ukradena ali izgubljena, se lahko izdaja za imetnika za nakup blaga in storitev osebno ali na spletu (Types of credit card fraud, 2016). Vse kartice, ki na kakršenkoli način preidejo v roke kriminalcev, lahko postanejo predmet zlorabe, saj jih storilci lahko uporabijo za dvig denarja oziroma plačilo blaga in storitev (Lamberger, 2009).

2.1.3 Zlorabe ponarejenih kartic

Po besedah Zupančičeve (1999, str. 219) so ponarejevalci plačilnih kartic sposobni pretvoriti osnovne bančne podatke v varnostne kode, ki jih prenesejo na ponarejene kartice. Oblikovanje ponarejene kartice je skupaj z izgubljenimi karticami predstavljajo največjo grožnjo v kartičnem prometu. Kriminalne združbe so ob tem bile sposobne ponarediti tudi osebne dokumente, s katerimi so dokazovali »istovetnost«. Goljufi so konstantno iskali nove in inovativne načine za ustvarjanje ponarejenih kartic (Bhatla et al., 2003). Ponarejanje kartic se lahko vrši na dva načina; s pravo kartico, na katero dodamo oziroma spremenimo podatke (spreminjanje podatkov ali magnetnega zapisa in reembosiranje pravih kartic), lahko pa izdelamo drugo kartico, tako da obstajata dve s popolnoma enakimi podatki (Lamberger, 2011). Tveganje za zlorabe izgubljenih, ponarejenih ter ukradenih kartic ne bo izginilo, dokler se ne bo zmanjšalo število prodajnih mest, kjer bodo goljufi te kartice lahko uporabljali. Izdajatelji so delež tovrstnih zlorab nekako že zakrpali s tehnologijo EMV, potrebno pa je še izboljšanje varnosti na področju CNP-zlorab (Crossman, 2015).

2.1.4 CNP-zlorabe

O CNP-zlorabah govorimo, kadar kartica ni fizično prisotna, torej pri nakupovanju na daljavo ali uporabi kartice v kibernetnem prostoru. Nakupovanje brez neposrednega stika s prodajalcem postaja zaradi hitrosti ter udobja vse bolj priljubljeno, vendar pa ima tudi številne pasti. Pri tovrstnem nakupovanju nam namreč ni treba navesti številke PIN¹, ne potrebujemo niti podpisa. Iz tega razloga je zloraba brez fizične prisotnosti kartice verjetno najlažja vrsta goljufije (Types of credit card fraud, 2016). Značilnost tovrstne goljufije je, da je storjena prek interneta, po pošti ali telefonu. CNP-zlorabe so trenutno najhitreje rastoča vrsta zlorabe plačilnih kartic v mnogih delih sveta. Zlorabe CNP so v Evropi v letu 2013 predstavljale kar 66 % zlorab (Payment cards, 2016; European Central Bank, 2015a). Tovrstne zlorabe so začele v EU naraščati predvsem po uvedbi standardov EMV, saj je bila zloraba fizične kartice ob njihovi uvedbi nekoliko otežena (Anderson & Murdoch, 2014; Payment cards, 2016).

2.2 Kje se dogajajo zlorabe

2.2.1 Zlorabe kartic na internetu

Razvoj interneta je bil zaradi svoje čezmejne narave hitro priložnost za zlorabe plačilnih kartic na enostaven način (Bhatla et al., 2003, str. 5). Vzroki, zaradi katerih prihaja do zlorab na internetu, so v večini primerov povezani s tehničnimi pomanjkljivostmi (slabi varnostni mehanizmi) in človekovo nepazljivostjo (Zupančič, 1999, str. 220).

¹ PIN – osebna identifikacijska številka.

Lažno predstavljanje (angl. *phishing*). To je vrsta goljufije, ki se je pojavila z elektronskim bančništvom in elektronskim poslovanjem. Cilj *phishing* napadov je pridobivanje občutljivih informacij (gesel, uporabniških imen in podatkov o računi internetnih uporabnikov) s pomočjo elektronske pošte in lažnih spletnih strani. Storilec se pretvarja, da je nekdo drug, in žrtev pod pretvezo prepriča o potrebi po posredovanju teh podatkov. Ukradene informacije so nato lahko uporabljene za elektronske transakcije oziroma za ponarejanje kartic. *Phishing* se pojavlja predvsem z lažnimi in vabljivimi elektronskimi sporočili z namenom, da bi pritegnili čim večje število ljudi (Pavia et al., 2012; Završnik, 2015, str. 48). *Phishing* napadi bodo v prihodnosti najverjetneje predstavljali največjo grožnjo varnosti plačilnih kartic, saj naj bi se takšna dejanja povečala prav zaradi izboljšanja varnosti pri fizični zlorabi kartice (Crossman, 2015). Najbolj množični in sofisticiran *phishing* napad v Sloveniji se je zgodil 23. januarja 2015, ko so uporabnike slovenskih bank želeli prepričati, da svoje podatke za dostop do elektronskega bančništva vpišejo na lažna spletna mesta (Pozor: najbolj množičen in sofisticiran phishing napad v Sloveniji, 2016).

Zvabljanje (angl. *pharming*). Gre za avtomatizirano zvabljanje, kjer se uporabnika v sistemu domenskih imen preusmeri na lažno spletno mesto. Postopek *pharminga* vključuje namestitev zlonamernega programa na posameznikov računalnik ali na strežnik, ki usmerja internetni promet. Uporabnik je tako kljub pravilnemu vpisu spletne strani preusmerjen na njeno kopijo in goljufo tako lahko posreduje pomembne podatke o svojem računu (Završnik, 2015, str. 48).

Škodljiva programska oprema (angl. *malware*). Napadalci lahko z namestitvijo škodljive programske opreme pridobijo pomembne informacije neposredno iz uporabnikovega računalnika. Tovrstna oprema snema vse pritiske na tipke in napadalci brez uporabnikove vednosti pridobijo veliko pomembnih podatkov (Šavnik, 2008).

Lažne spletne trgovine. V tovrstnih primerih gre za lažno spletno stran, ki je identična resnični, uporabnik spletne strani pa težko posumi, da je karkoli narobe, saj sta spletni strani na pogled povsem enaki. Uporabniki na lažne spletne strani vpišejo prave podatke, s čimer goljufo nevede posredujejo vse potrebne podatke za izvedbo zlorabe na drugi spletni strani (Bhatha et al., 2003).

Lažni prodajalci blaga po telefonu. V tem primeru pride do klica neznane osebe po telefonu, ki se izdaja za prodajalca z namenom, da pridobi pomembne podatke s kartice, kar bi mu omogočalo oddaljene nakupe (Šavnik, 2008).

Hekerski vdor v baze e-trgovcev. Nekateri trgovci pri uporabi elektronske trgovine po nepotrebnem shranjujejo podatke o plačilnih karticah strank ter jih s tem izpostavljajo nevarnosti, da hekerji vdrejo v bazo podatkov in prekopirajo kartice (Šavnik, 2008).

Zaščita kartic na internetu. Kot navaja Združenje bank Slovenije, smo vsi uporabniki poslovanja prek spleta izpostavljeni določenim tveganjem, ki pa se jim s poznavanjem varnega poslovanja lahko vsaj delno izognemo ter tako preprečimo nadaljnje zlorabe (Temeljna pravila varne uporabe kartic, 2015):

- »Na bančno ali trgovčevo spletno stran dostopajte z vnosom naslova v vaš spletni brskalnik.
- Nikoli ne dostopajte do spletne strani s povezave, prejete v e-sporočilu, in ne vnašajte osebnih podatkov.
- Bodite pazljivi na e-sporočila, ki jih niste zahtevali ali iskali, ali na klice, pri katerih vas sprašujejo po osebnih podatkih ali številkah kartic. Te podatke hranite varno.
- Pazljivi bodite pri razkrivanju kakršnihkoli osebnih informacij nekomu, ki ga ne poznate.
- Če ste v dvomih, je najboljšo mesto za pomoč in ravnanje, kako ostati varen na spletu, spletno mesto vaše banke ali hranilnice.
- Prek spleta plačujte le tistim ponudnikom, za katere veste, da so verodostojni, varni in imajo zagotovljene varnostne zaščite na svojih spletnih straneh. Varni spletni trgovci običajno uporabljajo varnostne standarde 3-D Secure, ki jih prepoznate po logotipu 'MasterCard SecureCode' ali 'Verified by Visa'.
- Če spletna stran ne uporablja varnostne zaščite 3-D secure in niste prepričani glede varnosti/verodostojnosti spletne strani, kjer želite opraviti plačilo, tega ne storite, dokler se ne prepričate, da je storitev varna.
- Prepričajte se, da se ob vstopu na spletno stran trgovca v spodnjem desnem kotu zaslona pojavi ikona zaklenjene ključavnice. V vrstici brskalnika, kjer je zapisan trgovčev spletni naslov, pa boste opazili, da se ta iz »http« spremeni v »https«, kar pomeni, da je vzpostavljena varna povezava.
- 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.
- Obvezno poskrbite, da je tudi naprava, prek katere opravljate spletni nakup, ustrezno zaščiten pred vdori, zlorabami in zlonamerno programsko opremo oziroma redno skrbite za varnostne popravke in nadgradnje elektronskih naprav, s katerimi plačujete. Redno preverjajte posebne – nove informacije in napotke, kako zaščititi vaš osebni računalnik in naprave ter sebe prek spleta.
- Posebej bodite pozorni, če uporabljate javne dostopne točke (knjižnice, kavarne) ali katerikoli osebni računalnik, ki ni vaš in nad katerim nimate nadzora. Pred odhodom vedno preverite, ali ste za seboj pobrisali vse osebne in občutljive podatke.
- Nikoli ne zapustite računalnika, ko ste varno povezani na spletno stran trgovca. Prepričajte se tudi, da ste se pravilno odjavili, ko ste končali nakup.«

2.2.2 Zlorabe na prodajnem mestu in na bančnem avtomatu

Snemanje magnetnega zapisa (angl. *skimming*). Pojavlja se na bankomatih in POS-terminalih. Pomeni proces, kjer se z določeno napravo nepooblaščen prekopiira podatke z magnetne kartice in včasih s pomočjo skrite kamere, dvojne tipkovnice na bankomatu tudi posname vnos osebne številke (PIN), ki pripada tej kartici. Na osnovi tako pridobljenih podatkov se izdela kopija kartice, ki se jo nato uporabi na bančnih avtomatih ali POS-terminalih (Kaj je *skimming*, 2016, Šavnik, 2008). Na POS-terminalih pride do snemanja večinoma v restavracijah, barih in na bencinskih črpalkah, kjer goljufivi zaposleni z nedovoljeno napravo izvedejo prepis magnetnega zapisa (Types of credit card fraud, 2016). Glede na to, da namestitev *skimming* naprave zahteva fizičen dostop do POS-terminala in je takšne oblike težko izvesti na masovni ravni, se kriminalci pogosto poslužujejo tudi škodljive programske opreme za POS-terminal in z brezžično tehnologijo oddajajo podatke storilcem (Završnik, 2015, str. 53).

Shimming. Angl. *shimmer* je naprava, ki je nameščena v notranjosti POS-terminala ali bančnega avtomata z namenom, da prestreže podatke med čipom in čitalnikom (npr. osebna številka računa in datum veljavnosti). Pridobljene podatke se tako s čipa presname na magnetno kartico. Po zatrevanju strokovnjakov sicer takšne ponarejene kartice ni mogoče uporabiti za zlorabe, saj imajo podatki na čipni kartici in podatki na magnetni kartici različne vrednosti za preverjanje pristnosti. Edina možnost zlorabe bi bila v primeru, da bi izdajatelj opustil preverjanje CVV (angl. *card verification value code*) pri odobritvi transakcije, ki pa je sicer obvezno, zato je za preprečevanje tovrstnih zlorab nujna ustrezna avtorizacija transakcije (Kitten, 2015).

Libanonska zanka. Pri tej vrsti zlorabe gre za pridobivanje številke PIN. Storilec se postavi v bližino bančnega avtomata in opazuje osebo, ki uporablja bankomat, z namenom, da bi pridobil njeno PIN-število. V režo bankomata pred tem namesti plastične trakove, ki jih imenujemo libanonska zanka. Bankomat ob poskusu dviga gotovine kartico zadrži. Imetnik kartice je prepričan, da je z bankomatom nekaj narobe, zato se odpravi do najbližje poslovalnice izdajatelja kartice. Kriminallec nato kartico, ki je ostala v bankomatu, odstrani in jo lahko v tem času že pošteno zlorabi, saj pozna tudi številko PIN (Types of credit card fraud, 2016; Lamberger 2011).

Izguba in tatvina plačilne kartice. Če kartico izgubimo, jo goljuf lahko uporabi za oddaljene nakupe; če je zraven priložena tudi številka PIN, pa jo lahko uporabi tudi na bančnem avtomatu in prodajnih mestih (Šavnik, 2008). V primeru, da prodajno mesto še ni opremljeno z najnovejšo tehnologijo, je mogoča zloraba tudi brez poznavanja številke PIN.

Dvakratno odčitavanje plačilnih kartic. To se dogaja zaradi primerov, ker trgovci pri plačilu prek POS-terminala odčitajo podatke prek čipa ali magnetnega zapisa na POS-terminalu, poleg pa še na lastnem bralniku, kjer se podatki prenesejo v računalniški

program blagajne, kar lahko predstavlja varnostno tveganje (Šavnik, 2008). Zloraba na prodajnem mestu se lahko zgodi tudi, ko oseba na prodajnem mestu nezakonito posreduje številko računa ali osebne podatke naprej goljufom (Bhatla et al., 2003).

Zaščita kartic na POS-terminalu. Po napotkih Združenja bank Slovenije (Temeljna pravila varne uporabe kartic, 2015) moramo biti imetniki plačilnih kartic pozorni na naslednje:

- »Pri plačevanju kartice nikoli ne izpustite iz svojega vidnega polja. Vedno nadzirajte celoten postopek plačevanja. V restavraciji naj natakar uporabi prenosni POS-terminal ali pa ga sami pospremite do plačilnega mesta.
- Pred vnosom PIN-številke oziroma pred podpisom potrdila o nakupu (POS-izpisek oziroma slip) obvezno preverite ustreznost zneska plačila.
- Ko opravljate katerokoli storitev (še posebej na bančnem avtomatu), pazite, da nihče ne vidi vaše PIN-številke, ki ste jo vnesli, in da so čakajoči za vami dovolj oddaljeni od vas. Če kdo stoji preblizu, ga prosite, naj se odmakne.
- Nikoli ne dovolite, da vam kdorkoli pomaga pri vnosu PIN-številke pri postopku plačevanja ali jo celo vnese namesto vas. Bodite pozorni, da oseba, ki vam zaračunava blago ali storitev, kartico vstavi oziroma potegne skozi POS-terminal samo enkrat. Ob neuspešni avtorizaciji zahtevajte potrdilo oziroma slip o neuspešno opravljenem postopku.
- Natančno preverite vse izpiske prometa in jih primerjajte s potrdili o nakupih. Le s primerjavo izpiska prometa s potrdilom o nakupu oziroma slipom lahko ugotovite svojo dejansko porabo.
- Ker potrdila o opravljenih nakupih včasih vsebujejo več podatkov o kartici, stara potrdila trajno uničite.
- Na prodajnih mestih ne podpisujte nikakršnih potrdil o nakupu, ki niso namenjena takojšnjemu plačilu blaga ali storitev in imajo vpisan vnaprejšnji datum, so brez zneska ali so celo popolnoma prazna.«

Zaščita kartic na bančnem avtomatu. Za varnost na bančnem avtomatu Združenje bank Slovenije (Temeljna pravila varne uporabe kartic, 2015) imetnikom svetuje naslednje:

- »Med uporabo bančnega avtomata ne sme nihče videti vaše PIN-številke. Priporočamo, da pri vpisovanju PIN-številke z obema rokama zastrete tipkovnico tako, da onemogočite morebitno snemanje vaše PIN-številke iz vseh kotov. Če kdo stoji preblizu, ga prosite, naj se odmakne.
- Bančni avtomat uporabljajte sami. Če ga ne znate uporabljati, ne sprejemajte pomoči mimoidočega, temveč se o uporabi raje poučite v svoji banki ali hranilnici.
- Kartico uporabljajte na tistih avtomatih, ki stojijo na obljudenem in dobro osvetljenem mestu.

- Če na bančnem avtomatu zaznate kakršnekoli spremembe ali odstopanja od običajnega videza ali delovanja bančnega avtomata (npr. kartico težje vstavite v avtomat, na avtomatu so naprave ali stvari, ki jih običajno ni, neobičajna postavitve kamer, neobičajna reža, v katero se vstavlja kartica, itd.), vzemite kartico iz bančnega avtomata in izberite drugi avtomat. O tem čim prej obvestite izdajatelja na telefonsko številko, ki je zapisana na kartici, ali policijo na številko 113.
- Do bančnega avtomata, nameščenega v zaprtem prostoru, pridete tako, da si vrata odprete s potegom kartice. Zapomnite si, da vam za odpiranje vrat nikoli ni treba vnesti PIN-števila. Če je na vratih naprava, ki od vas zahteva vnos PIN-števila, tega ne storite, ampak o tem obvestite banko ali hranilnico.
- Če vam bančni avtomat ne vrne kartice (zaradi ovire, nameščene na reži za sprejem kartice), ob ali na njem pa je nalepljeno navodilo, da ponovno vnesite PIN-število, tega ne storite. Enako velja, če vam ponoven vnos PIN-števila predlaga oseba, ki se nahaja v bližini in se predstavlja za bančnega delavca. V obeh primerih takoj obvestite najbližjo enoto banke ali hranilnice ali policijo na 113.
- Če vam bančni avtomat kljub odobritvi storitve ne izplača gotovine, najprej preverite stanje na svojem računu. Če je vaše stanje na računu nespremenjeno in je bila torej storitev neuspešna oziroma prekinjena, se je to zgodilo najverjetneje zaradi bankomata v okvari ali pomanjkanja gotovine v njem. Če pa ugotovite, da je vaše stanje na računu spremenjeno oziroma je bil želeni znesek odobren, a ne tudi izplačan, pa o dogodku nemudoma obvestite svojo banko ali hranilnico. V primeru suma zlorabe oziroma suma, da je v reži bankomata za izplačilo gotovine vstavljena ovira, pa počakajte pri bančnem avtomatu tako dolgo, da pride na kraj dogodka interventna služba vaše banke ali hranilnice oziroma policija. Če se to zgodi v tujini, o tem obvestite policijo in ravnajte po nasvetu policije.«

2.2.3 Zlorabe plačilnih kartic skozi zgodovino

V Tabeli 3 so prikazane oblike zlorab plačilnih kartic, ki so se dogajale v zadnjih treh desetletjih. Opažamo, da so zlorabe s področja posamičnih kriminalcev postale del globalne kriminalne združbe, kjer tarča niso več le posamezni imetniki, temveč celotna plačilna industrija na splošno.

Prav tako opazimo, da za zlorabe z izgubljenimi ali ukradenimi karticami ni bilo potrebno obsežno obvladati tehnologije, saj so zlorabe plačilnih kartic izvirale le iz priložnostnih krajev, medtem pa je obsežno tehnološko znanje najpomembnejše pri izvedbi zlorab plačilnih kartic v današnjem času.

Tabela 3: Prikaz razvoja zlorab plačilnih kartic po obdobjih

Leto	1980	1990	2000	2010	2015
Vrsta napadalcev	Posamezniki	Skupine	Lokalne kriminalne združbe	Globalne kriminalne združbe	Globalne kriminalne združbe
Tarča	Potrošniki	Manjši trgovci	Veliki trgovci	Izdajatelji	Plačilna industrija
Prevladujoča oblika zlorabe	Izgubljene, ukradene	Ponarejanje, skimming	Kraja identitete, lažno predstavljanje	Čezmejne kraje, CNP-zlorabe, 3D Secure zlorabe, zlorabe na bankomatih, ID-zlorabe	Čezmejne kraje, CNP-zlorabe, zlorabe na bankomatih, ID-zlorabe, zavljanje, hekerski vdor
Vrsta kartice	Potovalne in trgovske kartice	Premium kreditne kartice	Kreditne kartice	Vse vrste	Vse vrste
Potrebno znanje	Priložnostne kraje	Osnovno računalniško znanje	Tehnološko znanje	Predrznost, strokovno tehnološko znanje, notranje informacije, globalne povezave	Predrznost, strokovno tehnološko znanje, notranje informacije, globalne povezave

Vir: Payment cards and mobile, Card Fraud Report, 2015, str. 15, tabela 20.

2.3 Statistični podatki o zlorabah plačilnih kartic

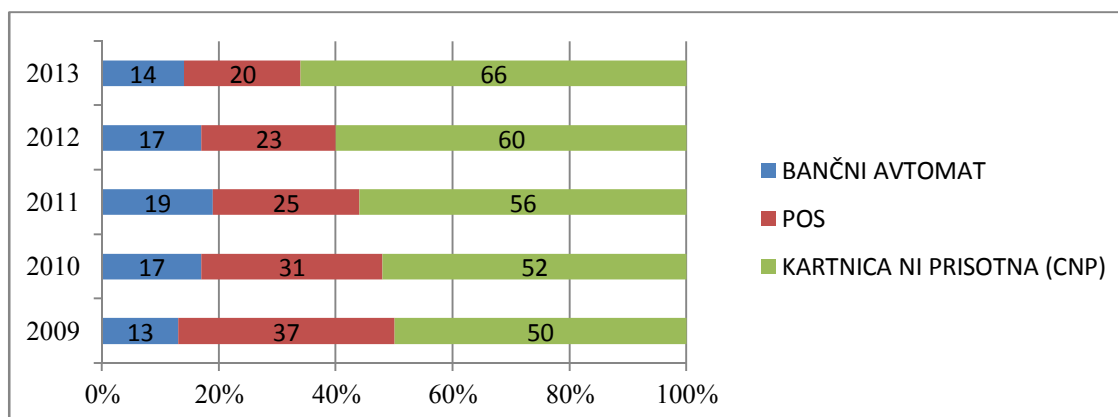
Pridobitev enotnih statističnih podatkov predstavlja nerešljiv problem. Razlog za to so neenotna opredelitev zlorab, pomanjkljive evidence, poslovne in bančne tajnosti.

2.3.1 Zlorabe plačilnih kartic v EU

Po podatkih ECB je bilo v EU v letu 2013 zlorabljenih 0,039 % plačilnih kartic, v ZDA pa kar 0,087 % (European Central Bank, 2015a).

Slika 5 prikazuje, kako so se med letoma 2009 in 2013 v EU spreminjali deleži po oblikah zlorab. CNP-zlorabe se v EU vsako leto večajo, v letu 2013 so predstavljale že 66 % vseh zlorab. Iz slike opazimo tudi zmanjšanje zlorab plačilnih kartic prek POS-terminala, medtem pa delež zlorab prek bančnega avtomata niha iz leta v leto.

Slika 5: Prikaz oblik zlorab, ki zavzemajo največje deleže v EU med letoma 2009 in 2013
v %



Vir: European Central Bank, Fourth report on card fraud, 2015, str.11, tabela A.

2.3.2 Zlorabe plačilnih kartic v Sloveniji

Za podatke o zlorabah plačilnih kartic v Sloveniji sem zaprosila policijo. Podatki policije so pomanjkljivi zato, ker policija vodi le tiste zlorabe, ki so ji bile prijavljene, ostalih pa ne, zato slika o zlorabah ni celostna.

V Tabeli 4 so najprej prikazani statistični podatki tatvine med letoma 2011 in 2015, kjer je bila predmet kraje tudi plačilna kartica.

Tabela 4: Statistika kaznivega dejanja tatvine v primerih, ko je bil ukraden predmet tudi plačilna kartica med letoma 2011 in 2015

Leto	2011	2012	2013	2014	2015
Število KD	2.452	2.487	1.905	2.053	1.555

Legenda: * Število KD pomeni število kaznivih dejanj.

Vir: Policija, M. Globelnic, osebna komunikacija, 21. marca 2016.

Iz Tabele 4 razberemo, da se je v letu 2015 število tovrstnih kaznivih dejanj izrazito zmanjšalo glede na leto prej. Po podatkih Policije gre pri tovrstnih kaznivih dejanjih najpogosteje za tatvine torbic ali denarnic, v katerih imajo oškodovanci spravljene tudi plačilne kartice. Podatkov o škodi, ki je nastala po tovrstnih tatvinah, predvsem v obliki dvigov ali uporabe ukradenih plačilnih kartic na prodajnih mestih, policija ne beleži (M. Globelnic, osebna komunikacija, 21. marca 2016).

V Tabeli 5 so prikazane zlorabe plačilnega sredstva glede na to, kako so goljufi prišli do podatkov, potrebnih za zlorabo.

Tabela 5: Statistika kaznivega dejanja uporabe ponarejenega plačilnega sredstva glede na način storitve med letoma 2011 in 2015

Način storitve	Vrednosti	Leto				
		2011	2012	2013	2014	2015
Ponarejanje plačilne kartice	Število KD	602	79	831	943	250
	Škoda v EUR	141.114	83.249	236.584	800.724	274.121
Pridobitev preko medmrežja	Število KD	85	93	658	105	149
	Škoda v EUR	73.361	87.229	64.804	48.813	90.175
Namestitvev naprav	Število KD	24	84	267	27	46
	Škoda v EUR	52.916	269.019	100.035	21.620	687.524

Legenda: * Število KD pomeni število kaznivih dejanj.

Vir: Policija, M. Globelnik, osebna komunikacija, 21. marca 2016.

Iz Tabele 5 razberemo, da je bilo s fizičnim ponarejanjem plačilne kartice največje število kaznivih dejanj storjeno v letu 2014, leto kasneje pa je upadlo. Pri zlorabah plačilne kartice, kjer so bili podatki pridobljeni prek medmrežja ali z namestitvijo naprav v letu 2015, zaznamo povečanje tovrstnih kaznivih dejanj glede na leto prej. V letu 2015 je bila v Sloveniji največja škoda povzročena z namestitvijo naprav in je znašala 687.524 EUR.

Tabela 6 prikazuje število kaznivih dejanj v primeru, ko je bila plačilna kartica zlorabljena na internetu.

Tabela 6: Statistika kaznivega dejanja goljufije v primerih, ko je bila plačilna kartica zlorabljena na internetu med letoma 2011 in 2015

Vrednosti	Leto				
	2011	2012	2013	2014	2015
Število KD	35	34	55	81	52
Škoda v EUR	19.345	32.749	13.315	33.279	17.150

Legenda: * Število KD pomeni število kaznivih dejanj.

Vir: Policija, M. Globelnik, osebna komunikacija, 21. marca 2016.

V letu 2014 smo v Sloveniji beležili največji porast števila kaznivih dejanj zlorabe plačilnih kartic, kjer je bila kartica zlorabljena na internetu, prav tako je bila tudi povzročena škoda v tem letu najvišja. V letu 2015 je Policija zaznala zmanjšanje tovrstnih zlorab glede na leto 2014, prav tako se je zmanjšala s tem povzročena škoda.

2.3.3 Zlorabe plačilnih kartic v Angliji

Tabela 7 prikazuje jasno sliko o zlorabah plačilnih kartic, ki so se dogajale v Angliji med letoma 2004 in 2014 in so razdeljene glede na obliko zlorabe.

Tabela 7: Letna izguba zaradi zlorab v Angliji med letoma 2004 in 2014 (v milijonih funtov)

Oblika zlorabe/ leto	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	Sprememba v letu 2014 glede na leto 2013 v %
CNP zlorabe	150.8	183.2	212.7	290.5	328.4	266.4	226.9	220.9	246.0	301.0	331.5	+10
Od tega e-trgovine*	117.0	117.1	154.5	178.3	181.7	153.2	135.1	139.6	140.2	190.1	217.4	+14
Ponarejene	129.7	96.8	98.6	144.3	169.8	80.9	47.6	36.1	42.1	43.4	47.8	+10
Izgubljene/ ukradene	114.4	89.0	68.5	56.2	54.1	47.9	44.4	50.1	55.2	58.9	59.7	+1
Kraja identitete	36.9	30.5	31.9	34.1	47.4	38.1	38.1	22.5	32.2	36.7	29.9	- 19
Nikoli prejete	72.9	40.0	15.4	10.2	10.2	6.9	8.4	11.3	12.8	10.4	10.1	-3
Skupaj	504.8	439.4	427.0	535.2	609.9	440.3	365.4	340.9	388.9	450.4	479.0	+6

Vir: Financial Fraud Action UK, Fraud The facts, 2015, str. 9.

Izgube zaradi zlorab plačilnih kartic so v letu 2014 v Angliji znašale 479 milijonov funtov, kar predstavlja skupno 6 % rast glede na leto prej. Največje zmanjšanje zlorab skoraj pri vseh oblikah opazimo v letu 2009, kar gre prav gotovo pripisati uvedbi standarda EMV in prilagajanju kriminalcev, da se standardu prilagodijo. Iz tabele se lepo vidi, kako se je način zlorab plačilnih kartic z leti spreminjal. V letu 2008 je bilo še največ zlorab s ponarejenimi karticami, v letu 2014 pa daleč največji delež zavzemajo CNP-zlorabe. Največji upad zlorab glede na obliko v zadnjih letih je beležen s ponarejenimi karticami.

3 VARNOST IN STANDARDI

Po navedbah Zupančičeve (1999, str. 220) so za boj proti zlorabam potrebni zanesljivost delovanja, standardizacija programske opreme in uporabljenih protokolov ter varnostni mehanizmi.

3.1 Plačilne kartice po obdobjih

Prve plačilne kartice so bile natisnjene na papirju, kar je omogočalo le najnižjo stopnjo varnosti. Nadalje so pričeli z izdajanjem kovinskih kartic, pri čemer so bili podatki vtisnjeni s pomočjo embosiranja. Podatki so vsebovali le najosnovnejše podatke o imetniku (ime in priimek, datum veljavnosti in številka računa). Skozi zgodovino tako spremljamo številne izboljšane vidike varnosti, zato so kovinske kartice hitro zamenjale plastične kartice. Številko računa na plastičnih karticah so pričeli izpisovati reliefno, s čimer je bil storjen prvi korak k avtomatizaciji plačevanja (Zelenik & Mezgec, 2009; Woolsey et al., 2009; Lamberger et al., 2012).

3.1.1 Magnetna kartica

Kartica, opremljena z magnetnim zapisom, je nastala zaradi potrebe po avtomatizaciji v bančništvu, s tem, da so navadni plastični kartici dodali še magnetni trak (Zupančič, 1999). V veljavo je stopila leta 1970 (Anderson & Murdoch, 2014). V magnetnem zapisu so skriti vsi podatki o imetniku kartice in izdajatelju (Lamberger, 2009, str. 29). Magnetna kartica vsebuje zelo slabe varnostne standarde, saj vsebuje le šibko statično kodo za preverjanje pristnosti, poleg tega pa podatki niso šifrirani, zato jih ni težko ponarediti oziroma ukradene ali izgubljene kartice zlorabiti. S pridobljenimi podatki z magnetne kartice in nekaj ustrezne opreme (računalnik in naprava, ki bere magnetni zapis) je moč na dokaj enostaven način kartico ponarediti in zlorabiti (Sullivan, 2013).

3.1.2 Tehnologija po standardu EMV

Ker se varnost magnetnih kartic, ki so bile v rabi skoraj pol stoletja, z leti ni nič izboljšala, so kartice z magnetnim trakom začele nadomeščati pametne kartice z integriranim vezjem – čipne kartice (Zelenik et al., 2009). Tovrstne kartice delujejo na skupnem standardu, imenovanem EMV, ki pomeni uveljavljen svetovni standard za kreditne in debetne kartice, ki temelji na čipni tehnologiji. Njegove funkcije so: **preverjanje pristnosti**² čipne kartice, kar zagotavlja, da je izdajatelj izdal kartico ter da se podrobnosti na njej niso spremenile; **preverjanje imetnika kartice**³, kar zagotavlja, da je imetnik upravičen do rabe kartice; **avtorizacija**⁴ transakcije, kar zagotavlja, da ima imetnik dovolj sredstev za plačilo transakcije (Alhothaily, Alrawais, Cheng, & Bie, 2015). Standard EMV je nastal leta 1994 kot rezultat skupnega dela vodilnih institucij na področju plačevanja (Europay, MasterCard in Visa) z namenom zagotavljanja varnosti plačil na globalni ravni. Danes je globalna znamka EMV v lasti 6 članic EMVCo: American Express, Discover, UnionPay, JCB, MasterCard in Visa (Kobs, 2015).

Glavni razlogi za vpeljavo EMV-standarda so bili v namenu zmanjšanja zlorab ponorejenih, izgubljenih ter ukradenih kartic, saj se ta tehnologija šteje za veliko bolj varno, ker uporablja napredne varnostne funkcije, ki naj bi onemogočale zlorabe. Standard EMV pomaga zaščititi morebitna plačila na prodajnem mestu z ukradenimi ali s ponorejenimi karticami. Na čipu so shranjeni podatki o računu in osebni podatki, ki so potrebni za uporabo kartice. Razlika pri uporabi magnetne in čipne kartice se kaže v tem, da se jo pri plačilu na prodajnem mestu ne povleče prek bralnika kakor magnetno, temveč se jo vanj vstavi. Čip se poveže z bralnikom in tako omogoči izvedbo izmenjave podatkov,

² Kartična prepoznavnost (angl. *Card Authentication*) – funkcija, s katero lahko procesor ali izdajatelj prepozna kartico (ZBS, 2011, str. 14).

³ Preverjanje imetnika kartice (angl. *Cardholder Verification*) – izdajatelj ali procesor lahko s pomočjo verifikacije preveri imetnika kartice (ZBS, 2011, str. 15).

⁴ Avtorizacija (angl. *Authorisation*) – avtorizacija je uporabljena s strani prejemnika transakcije/imetnika za odločanje o izvedbi (odobritvi oziroma zavrnitvi) transakcije. Glede na tip čipa, nameščenega na kartici, se avtorizacija lahko opravi na 'on-line' ali 'off-line' način. V primeru on-line avtorizacije obstaja tudi možnost delne odobritve (avtorizacije) transakcije (ZBS, 2011, str. 14).

kar imenujemo kontaktna transakcija (Kobs, 2015; Marshall & Latin, 2015). Kartica EMV zahteva tudi uporabo PIN-številke za vsako transakcijo, zato jo pogosto imenujemo kar ČIP&PIN kartica (Sullivan, 2009).

Kot dober primer vpeljave standarda EMV naj navedemo, da so se zlorabe plačilnih kartic v Franciji znižale kar za 80 % (Ruark, 2015). Vpeljava standarda EMV pomeni tudi premik odgovornosti, saj so izdajatelji pred njegovo uvedbo bili odgovorni za vsako zlorabo na prodajnem mestu, od uvedbe naprej pa se odgovornost seli na prodajalce, če prodajno mesto (POS-terminal) ni opremljeno po tehnologiji EMV. Podjetja, ki sprejemajo plačilne kartice in še niso posodobila plačilnih terminalov, so tako postala potencialno odgovorna za zlorabe, prej pa so bila od odgovornosti večinoma izolirana. Standard je v EU obvezen že nekaj let, v ZDA pa se je množično prilagajanje pričelo konec leta 2015 (Marshall et al., 2015; Kobs, 2015).

Problem čipnih kartic pa obstaja, ker še vedno vsebujejo tudi nešifriran magnetni zapis. Zaradi globalno še ne vpeljane tehnologije po standardu EMV se magnetni zapis na karticah namreč ohranja. V primeru, da nepridipravi dobijo številko PIN, lahko kartico še vedno ponaredijo in zlorabijo. Prav tako obstaja možnost lažne transakcije. Goljuf npr. lahko postavi lažni parkomat, da ukrade podatke, medtem pa lahko pajdaš plačuje prek ponarejene kartice tako, da je povezan z lažnim parkomatom, ki mu pošilja podatke o žrtvini kartici. Naslednja zanimiva prevara se zgodi, če je ukradena kartica uporabljena brez poznavanja številke PIN. To lahko goljuf stori tako, da med terminal in kartico postavi majhno elektronsko napravo, ki mu omogoča, da vpiše katerokoli številko PIN, sistem pa jo sprejme kot pravilno (Anderson et al., 2014). Po poročanju Monitorja so nepridipravi izdelali tudi prilagojene kartice, ki so bile le nekoliko debelejšje od pravih in niso zbujale pozornosti, saj jih je bilo še vedno mogoče vstaviti v bralnik. Dodali so jim poseben čip, ki je prestregel vtiskani PIN in terminal pretental v izvedbo transakcije. PIN je torej prestregel drugi čip in terminalu vrnil pravilni rezultat ne glede na to, ali je bil vneseni PIN pravilen ali ne ("Nov" način zlorabe plačilnih kartic, 2015).

Prilagajanje v ZDA. Največ zlorab plačilnih kartic se zgodi v ZDA. Večina strokovnjakov meni, da se v ZDA zgodi toliko zlorab prav zaradi počasne vpeljave standarda EMV (Holmes, 2015). Strožje preverjanje imetnika in kartice naj bi tudi v ZDA vodilo v zmanjšanje zlorab plačilnih kartic (Kobs, 2015). Ključni dejavnik, ki je v ZDA zaviral varnostni napredek kartičnega poslovanja, je tako imenovani učinek kokoši in jajca (angl. *chicken and egg effect*). Izdajatelji niso želeli preveč hiteti z izdajanjem EMV-kartic, saj so vedeli, da trgovci še niso pripravljeni, kar bi pomenilo, da stranke kartic ne bi mogle uporabljati. Naslednji razlog je bil tudi v prepočasni nadgradnji vseh procesorjev, ki bi tako ovirali potek transakcije. Na drugi strani pa se trgovci niso želeli posluževati novih POS-terminalov, saj so bili stroški precejšnji; poleg tega pa se niso zavedali, kakšni so stroški zlorab, glede na to, da prej za morebitne zlorabe niso nosili odgovornosti (Crossman, 2015). Po besedah Murdoch et al. (2014) bo trajalo še nekaj let, preden bo v

ZDA prišlo do popolne zamenjave magnetnih kartic, saj je treba nadgraditi vse bankomate in POS terminale. Po ustrezni namestitvi bo tudi vidno morebitno zmanjšanje zlorab zaradi uvedbe EMV. Izdajatelji plačilnih kartic v Evropi in Kanadi so prodajalce motivirali za uvedbo EMV predvsem zaradi premika odgovornosti, saj so banke svoje pogoje spremenile tako, da so prodajalcem naložile odgovornost za vse morebitne goljufive transakcije, če so te opravljene brez PIN-številke (Anderson et al., 2014).

3.1.3 Brezstična tehnologija

Izdajatelji plačilnih kartic razvijajo vedno nove načine za izvedbo plačil. Med novejšje primere spada tudi tehnologija NFC (angl. *near field communication*). Brezstična pametna tehnologija temelji na varnem mikročipu, ki omogoča varno upravljanje in hrambo podatkov, ter anteni, ki omogoča komuniciranje prek radijske frekvence s POS-terminalom. Tehnologija omogoča imetniku, da opravi nakup brez vstavljanja kartice v POS-terminal, namesto tega jo napravi samo približa, s čimer je transakcija opravljena. Do določenega zneska prav tako ni treba vnesti osebne številke PIN. Glavni namen tovrstnih kartic naj bi bila hitrejša izvedba plačil na prodajnih mestih, zato jim včasih rečemo tudi potegni in pojdi kartice (angl. *tap&go*) (Kobs, 2015; The What, Who and Why of Contactless Payments, 2016). Prednosti brezstične kartice za uporabnike (Združenje bank Slovenije, 2016):

- **hitrost;** pospeši postopek plačevanja pri plačilih majhne vrednosti;
- **varnost;** uporabnik svoje kartice nikoli ne izpusti iz rok. Plačila višjih vrednosti zahtevajo vnos številke PIN, limit porabe brez številke PIN pa je omejen za nakup do 15 EUR. Po zaslugi številnih varnostnih mehanizmov je brezstična transakcija varnejša od klasičnega plačevanja s kartico. Brezstični del čipa vsebuje minimalno količino podatkov. Na čipu je tudi kriptogram, ki omogoča šifriranje podatkov. Za vsako transakcijo je znano, ali je bila izvedena stično ali brezstično;
- **praktičnost.**

Prednosti brezstičnih kartic za trgovce pa so v zmanjšanju blagajniških procesov, hitrosti in priročnosti, ki omogoča učinkovitejšo prodajo in posledično več prihodkov (Združenje bank Slovenije, 2016).

Naprave za izvedbo zlorab brezstičnih kartic pa so dokaj poceni, saj je mogoče že za nekaj 100 dolarjev kupiti potrebno opremo za krajo podatkov. Goljuf tako lahko npr. že ob hoji poleg žrtve nevidno, brezzično skozi denarnico, torbico ali žep ukrade podatke s kartice. Zlasti so nevarni prostori, kjer se zadržuje veliko število ljudi (letališča, nakupovalni centri, športne prireditve), saj je napravo mogoče tudi neopazno skriti. Izdajatelji tovrstnih plačilnih kartic sicer vztrajno zanikajo, da je mogoče podatke z njih enostavno, poceni in nepričakovano pridobiti ter jih uporabiti za goljufive namene, in podcenjujejo tveganje, povezano s to tehnologijo (Greenberg, 2015; Brody et al., 2014).

3.2 Skrb za varnost

Pri iskanju varnostnih rešitev za varovanje plačilnih kartic se srečamo z vrsto standardov, med katerimi je najpomembnejši PCI-standard. To je pravzaprav produkt največjih kartičnih izdajateljev za varnejše in sistematizirano poslovanje pri uporabi plačilnih kartic. Vsebuje zbirko obveznih priporočil, ki jih morajo upoštevati vsi, ki uporabljajo kartične storitve; pravne osebe (trgovci in ponudniki storitev), izdajatelji kartic in drugi z namenom vzpostavitve varnega informacijskega sistema, kjer bodo podatki in informacije o plačilnih karticah zaščiteni (Lamberger et al., 2012; PCI DSS Quick Reference Guide, 2014).

3.2.1 PCI-standardi

Payment Card Industry Security Standards Council (v nadaljevanju PCI SSC) je bil ustanovljen septembra 2006 na pobudo vodilnih izdajateljev plačilnih kartic (American Express, Discover, JCB International, MasterCard in Visa Inc.). Njegov namen je omejitev tveganja in zagotavljanje: varnega poslovanja s plačilnimi karticami za imetnike kartic; varnega poslovanja s plačilnimi karticami za trgovce; izogibanja finančnim tveganjem; izogibanja tveganjem izgube ugleda in skladnosti z zakonodajo (Glas, 2012, str. 9–10). Postal je koordinator za varnostne standarde kartičnega poslovanja. Glavni cilj je bil zaščita kartičnega poslovanja in posledično zmanjšanje zlorab plačilnih kartic. PCI SSC izdaja tri glavne sklope standardov:

- **PCI PA DSS** (angl. *Payment Application Data Security Standard*) je namenjen razvoju varne programske opreme za obdelavo transakcij plačilnih kartic. Zahteve v tem standardu opredeljujejo predvsem varnost programske opreme skozi faze razvoja, uvedbe in vzdrževanja (Glas, 2012, str. 3; PCI DSS Quick Reference Guide, 2014);
- **PCI PTS** (angl. *PIN Transaction Security Requirements*) je namenjen razvoju varne strojne opreme za zajem podatkov, ki so potrebni za izvedbo transakcije s plačilno kartico. Standard natančno opredeljuje tehnično-tehnološke zahteve za varen zajem in prenos najbolj kritičnih podatkov v procesu kartičnega poslovanja, kot so PAN (številka kartice), PIN (osebna številka), zapis z magnetne steze ali čipa (Glas, 2012, str. 3; PCI DSS Quick Reference Guide, 2014);
- **PCI DSS** (angl. *Payment Card Industry Data Security Standard*) je globalni varnostni standard, ki usmerja standardizirano poslovanje. Upoštevati ga morajo vsi, ki zajemajo, obdelujejo, hranijo ali posredujejo podatke o plačilnih karticah in njihovih imetnikih. Namenjen je vsem subjektom, ki so vključeni v obdelavo plačila s karticami, vključno s trgovci, procesorji, izdajatelji in pridobitelji (PCI DSS Quick Reference Guide, 2014, str. 7; Glas, 2012, str. 2). PCI DSS je namenjen upravljanju varovanja informacij o karticah v finančnih institucijah, procesnih centrih in pri trgovcih. Sestavljen je iz zahtev, ki predvidevajo implementacijo tehnično-tehnoloških rešitev in implementacijo organizacijsko formalnih rešitev (Glas, 2012, str. 3).

PCI DSS je sestavljen iz šestih načel, ki so nadalje razdeljena na 12 zahtev, ki so naložene udeležencem v plačilnem procesu, kar nazorneje prikazuje Tabela 8.

Tabela 8: Načela PCI DSS

Načelo	Zahteva
Vzpostavitev in vzdrževanje varnega omrežja	Zahteva št. 1 – vzpostaviti in vzdrževati konfiguracijo požarne pregrade Zahteva št. 2 – ne uporabljati privzetih nastavitev, ki jih dobavi prodajalec sistema, za sistemska gesla in druge varnostne parametre
Varovanje podatkov o imetniku plačilne kartice	Zahteva št. 3 – zavarovati shranjene podatke o imetniku plačilne kartice Zahteva št. 4 – šifriranje prenosa podatkov o imetniku plačilne kartice prek odprtih, javnih omrežij
Vzdrževati program za upravljanje z ranljivostmi sistema	Zahteva št. 5 – uporabljati in redno posodabljati protivirusno programsko opremo ali programe Zahteva št. 6 – razvijati in vzdrževati varne sisteme in aplikacije
Implementacija ukrepov za kontrolo dostopa do občutljivih kartičnih podatkov	Zahteva št. 7 – omejitev dostopa do podatkov o imetniku plačilne kartice na najmanjši obseg, ki je potreben za izvršitev transakcije Zahteva št. 8 – dodeliti edinstveno identifikacijsko številko vsaki osebi, ki ima dostop do informacijske podpore Zahteva št. 9 – omejiti fizični dostop do podatkov o imetniku plačilne kartice
Redno spremljanje in testiranje omrežij	Zahteva št. 10 – slediti in nadzorovati vse dostope do omrežnih virov in do podatkov o imetniku plačilne kartice Zahteva št. 11 – redno testiranje varnostnih sistemov in procesov
Vzdrževanje politike varovanja informacij	Zahteva št. 12 – vzdrževati politiko, ki ureja področje varnosti informacij ter velja za zaposlene in pogodbene izvajalce

Vir: PCI Security Standard Council, PCI DSS Quick Reference Guide, 2014, str. 7; A. Glas, Varnost kartičnega poslovanja – PCI DSS - payment card industry data security standard, 2012, str. 3.

Če se malo bolj poglobimo v zahtevo št. 3, ugotovimo, da zahteva, da se ne sme hraniti občutljivih podatkov za preverjanje pristnosti, vključno s podatki magnetnega zapisa, CVC ter številke PIN. Poleg tega je treba številko kartice (PAN) šifrirati, da postane neberljiva (Calder & Carter, 2008).

Tabela 9 ponazarja občutljive podatke za preverjanje pristnosti imetnika kartice, za katere podatke je dovoljena hramba in ali je zahtevana zaščita teh podatkov. Občutljivi podatki za preverjanje pristnosti se nikakor ne smejo hraniti po avtorizaciji (PCI DSS Quick Reference Guide, 2014).

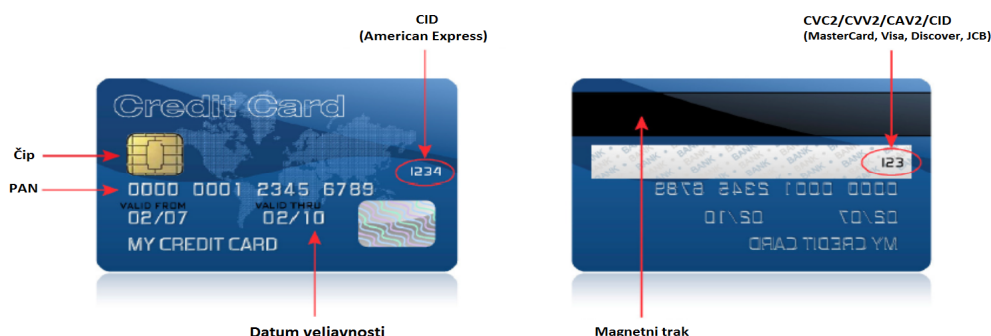
Tabela 9: Varovani podatki po PCI DSS

	Podatek	Dovoljena hramba	Zahtevana zaščita	Šifriranje podatkov
Podatki o plačilni kartici	Številka kartice (PAN)	DA	DA	DA
	Naziv imetnika plačilne kartice	DA	DA	NE
	Service Code	DA	DA	NE
	Rok veljavnosti	DA	DA	NE
Občutljivi podatki o odobritvi plačila	Podatki celotnega magnetnega zapisa	NE	/	/
	CVC2/CVV2/CID/CAV2	NE	/	/
	PIN/PIN block	NE	/	/

Vir: PCI Data Security Standard, Requirements and Security Assessment Procedures. Version 3.1, 2015, str. 8; A. Glas, Varnost kartičnega poslovanja – PCI DSS (payment card industry data security standard), 2012, str. 3.

Za lažjo predstavbo, kje se vsi ti podatki nahajajo, so na Sliki 6 prikazani plačilna kartica in podatki na njeni površini.

Slika 6: Podatki, ki so vidni na plačilni kartici



Vir: PCI DSS Quick Reference Guide, 2014, str. 11.

V Tabeli 10 prikazujem, za preprečevanje katere vrste zlorab je standard učinkovit.

Tabela 10: Učinkovitost PCI DSS pri preprečevanju zlorab plačilnih kartic

Tip zlorabe	Način kraje podatkov	PCI DSS zahteva
CNP	Vdor v informacijski sistem trgovca, procesnega centra, banke ipd.	Vse zahteve PCI DSS
Kraja identitete	Kraja podatkov pri imetniku plačilne kartice	Ni primerno, drugi načini zmanjševanja tveganj (ozaveščanje imetnikov kartic)
Skimming	POS	2,8,9,10,12

se nadaljuje

Tabela 10: Učinkovitost PCI DSS pri preprečevanju zlorab plačilnih kartic (nad.)

Tip zlorabe	Način kraje podatkov	PCI DSS zahteva
Skimming	ATM	Ni primerno, drugi načini zmanjševanja tveganj (antiskimming naprave)

Vir: A. Glas, Varnost kartičnega poslovanja – PCI DSS (payment card industry data security standard), 2012, str. 9.

3.2.2 Tokenizacija

Je pravzaprav dopolnilo standarda EMV, saj s pomočjo dinamičnih podatkov preprečuje morebitne goljufije. EMV kot tak ne šifrira podatkov, zato je za zaščito podatkov potrebna tokenizacija. Tokenizacija pomeni zamenjavo oziroma zaščito zaupnih podatkov z nadomestno vrednostjo. Izvira iz angl. besede *token* in pomeni žeton. Varnostno občutljiv podatek se torej ne pojavlja v podatkovnih bazah in transakcijah, ampak se uporabi žeton, kar pomeni neke vrste sklic do originalnih podatkov. Tokenizacija torej zmanjša tveganje v primeru vdora v informacijski sistem in zagotavlja še dodaten sloj varnosti, ki poteka v ozadju (RSA, 2014; Lubej, 2014).

3.2.3 Secure code

Znatne investicije in prizadevanja vseh operaterjev za zagotovitev prehoda s tehnologije magnetnega traku na tehnologijo EMV so pozitivno vplivale na zmanjšanje obsega kartičnih goljufij v okolju, kjer je plačilna kartica fizično prisotna. Trendi pa so pokazali, da je največje tveganje goljufij povezano prav s kartičnimi transakcijami na daljavo (Evropski ekonomsko-socialni odbor, 2012). Veliko zlorab kreditnih kartic se zgodi zaradi neustreznega hranjenja podatkov trgovcev. Spletni trgovec se namreč lahko odloči, da bo kupcem omogočil vnovičen nakup na spletni strani brez vnašanja podatkov o plačilni kartici. Da je to sploh mogoče, mora trgovec potrebne podatke hraniti. Standard PCI DSS pa hrambo CVC-kode striktno prepoveduje, saj je to koda, ki se uporablja za preverjanje istovetnosti lastnika in je dostopna samo njemu. Ker pa del trgovcev ne upošteva načela o hrambi podatkov, s tem ogroža svoje kupce. Transakcija je izvedena tako, da spletna trgovina vzpostavi povezavo z banko oziroma s transakcijskim strežnikom. Ta lahko v realnem času preveri veljavnost plačilne kartice. V primeru vdora v spletno trgovino je najbolje, da trgovec uporablja kriptografske metode, ki onemogočajo prosto berljivost in dešifriranje. Za boljšo varnost poskrbijo tako, da je poslovanje standardizirano po katerem izmed uveljavljenih standardov – npr. PCI DSS, saj ta striktno določa kriptiranje vseh bistvenih podatkov na kartici, vključno s kodo CVC, ter zahteva kodirano povezavo s strežniki (Žagar, 2011, str. 22–25). Leta 2001 je družba Visa prva predstavila dodatno raven varovanja z uvedbo storitve »Verifeid by Visa«, podprto s standardom 3-D Secure, kmalu pa sta se ji pridružila tudi Mastercard s standardom »Mastercard Secure-Code« ter American Express s standardom »SafeKey« (RSA, 2014; 3D Secure, 2016).

Danes omogočanje sprejema varnih načinov preverjanja pristnosti omogoča skupni standard 3-D Secure (3-D *Secure Cardholder Authentication Scheme*), mednarodni varnostni standard, ki se uporablja za preverjanje istovetnosti uporabnikov kartic pri spletnem plačevanju. Je last družb Visa, MasterCard in Amexa. Razvit je bil z namenom zmanjšanja tveganj nepooblaščne rabe kartic s strani tretjih oseb, s čimer bi pripomogel k rasti elektronskega plačevanja. Kot navaja MasterCard (2016), so koristi 3-D Secure: zaščita imetnika pred nepooblaščno uporabo; dodatna varnost pred zlorabami; premik odgovornosti; povečanje zaupanja kupcev in varnost ter zanesljivost. Visoka stopnja varnosti se zagotavlja z zahtevo po dodatnem preverjanju pristnosti plačila. Cilj je zagotoviti varno in zanesljivo spletno plačilo s pomočjo gesla, ki je potrjeno s strani izdajatelja kartice. »Protokol ob aktivaciji in vsaki poznejši uporabi na spletnem prodajnem mestu preveri pristnost imetnika kartice. To poteka tako, da vsakokrat primerja vnesene podatke v pojavnih oknih s podatki, ki so shranjeni na varnem strežniku. Aktivacija in nadaljnja uporaba sta uspešni zgolj v primeru pravilno vnesenih podatkov« (Dulc & Strahinič, 2014). Vpeljava 3-D Secure zaščite je ključna za zmanjšanje CNP-zlorab. Poleg tega omogoča tudi prenos odgovornosti na pridobitelja v primeru, da ta nima ustrezne zaščite, ki omogoča varno uporabo (RSA, 2014, str. 9; 3D Secure, 2016).

3-D Secure lahko aktiviramo že ob prvem nakupu prek spletne strani, ki omogoča ta standard. Za delovanje uporablja arhitekturo treh domen in je zasnovan na SSL-tehnologiji (angl. *Secure Socket Layer*), ki zagotavlja kodiranje ter varno izvedbo spletne transakcije. Med prenosom omogoča zaščito podatkov na plačilni kartici in preverjanje pristnosti vseh vpletenih (Rizmal, 2008, str. 12):

- domena izdajatelja je odgovorna za pravilen in varen vpis podatkov ter avtentikacijo imetnika;
- domena pridobitelja zagotavlja, da prodajno mesto v transakciji deluje v okviru sporazuma in skrbi za dejanski potek transakcije;
- domena interoperabilnosti omogoča izmenjavo transakcij med ostalima dvema domenama.

3.2.4 Ostali načini preprečevanja zlorab

Za omejitev zlorab morajo sodelovati trgovci, izdajatelji plačilnih kartic, zakonodajalec, varnostni standardi, veliko pa moramo prispevati tudi imetniki sami. Tako izdajatelj kot imetnik kartice sta zainteresirana za zgodnje opozarjanje in preprečevanje nepravilne uporabe kartice, da se prepreči ekonomske posledice, ki bi jih zloraba lahko povzročila. Odkrivanje prevar z varovalnimi mehanizmi in analizami porabe je za izdajatelje pomemben del procesa zaščite. Izdajatelji zato počnejo vse, kar je v njihovi moči s čimprejšnjim obveščanjem imetnika, če zlorabo zaznajo. V veliko primerih izdajatelji zlorabo zaznajo pred imetnikom samim. A tudi izdajatelji se zavedajo, da je problem goljufij kartic, da so lahko hitre, enostavne in neopazne, predvsem v primeru manjših izgub

(Brody et al., 2014). Po besedah Cheney et al. (2012) bi se stroški izgub z zlorabljenimi karticami sicer zmanjšali s še višjimi varnostnimi standardi, vendar se je treba zavedati, da goljufij ni mogoče povsem odpraviti.

Imetnik kartice in izdajatelj se lahko v pogodbi dogovorita o omejitvi porabe za določeno plačilno kartico. Obstaja omejitev odgovornosti imetnika za izgubo do največ 150 EUR, zato sta z vidika izdajatelja pomembna ukrepa omejevanje posledic neodobrenih plačilnih transakcij in enostranska blokada plačilnega instrumenta (Kovač, 2011, str. 59–60). Po pregledu splošnih pogojev različnih izdajateljev kartic ugotavljam, da izdajatelj v večini primerov blokira kartico, ko:

- obstaja možnost, da plačilnih transakcij ne opravlja uporabnik kartice, ampak nepooblaščen oseba,
- obstaja možnost, da je nepooblaščen oseba pridobila podatke o kartici,
- bankomat uporabniku odvzame kartico,
- uporabnik kartice trikrat napačno vtipka PIN-številko na bankomatu ali POS-terminalu.

D'Arcy, Hovan in Galletta (2009) pravijo, da je za zmanjšanje ogroženosti v kibernetnem prostoru treba sprejeti naslednje varnostne ukrepe:

- povečanje uporabnikovega poznavanja mogočih groženj,
- izobraževanje o varnosti in
- ozaveščanje o samovarovanju.

Podjetja in finančne institucije odgovornost do zaščite osebnih podatkov kažejo tudi z zavedanjem kibernetnega tveganja. Pred tveganjem zlorabe osebnih podatkov zaradi hekerskega vdora v računalniški sistem ter odgovornosti elektronskega plačevanja obstaja možnost kibernetnega zavarovanja, ki ponuja kritja na različnih področjih informacijskega tveganja. Izdajatelji plačilnih kartic morajo v prvi vrsti sicer uresničiti načrte za zmanjšanje nevarnosti, poleg tega pa se osredotočati tudi na uporabo kibernetnega zavarovanja kot pomembnega člena (Giblin, 2015).

Ukrepi za varnost plačilnih kartic temeljijo predvsem na tehnoloških ukrepih, ki so vpeti v proces transakcije (povečevanje varnostnih standardov, zaščitna programska oprema in zapletena kriptografija). Izdajatelji so zato pričeli tudi z novo obliko, kjer ima vlogo preprečevanja zlorab tudi imetnik kartice, saj ga izdajatelj lahko bodisi obvesti o transakciji prek sporočila SMS oziroma se skupno dogovorita o omejitvi porabe za nekatere vrste nakupov oziroma do določene višine limita (Quah & Sriganesh, 2008). Kot menijo Pavia et al. (2014), bi bil boj proti zlorabam z aktivnim sodelovanjem imetnika najbolj uspešen, vendar je to odvisno od njegove pripravljenosti ter od tega, koliko izdajatelji lahko zaupajo imetnikom. Imetnik plačilne kartice je po zakonu dolžan uporabljati plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega

instrumenta, in takoj po prejemu plačilnega instrumenta zlasti zagotoviti vse razumne ukrepe, da zavaruje varnostne elemente plačilnega instrumenta, ki omogočajo identifikacijo uporabnika in so vezani osebno nanj (ZPlaSS, 16. člen).

Glede na razširjenost uporabe plačilnih kartic imajo goljufi veliko možnosti. Obstajajo številni preventivni ukrepi, ki bi se jih morali zavedati vsi, da bi zmanjšali možnost zlorabe. Podjetja bi se morala zavedati, da bi bilo treba omejiti podatke, ki jih hranijo, na tiste bistvene poslovne informacije, s čimer bi se zmanjšala količina podatkov, do katerih lahko pridejo goljufi. Nadalje je treba vlagati v učinkovite požarne zidove in ustrezno programsko opremo. Imetnik mora biti previden pri plačevanju in pozoren na vsakršno sumljivo vedenje osebja. Pri plačevanju na spletnih straneh mora biti pozoren, da je spletna stran varna, brezstično kartico pa lahko za večjo varnost zavije v folijo (Brody et al., 2014).

4 ZAVAROVANJE ZLORAB PLAČILNIH KARTIC

Varnost je ena od človekovih temeljnih potreb. V zavarovalništvu se pojavlja kot produkt, dobrina, ki jo zavarovalnice tržijo svojim kupcem (Žnidarič, 2004, str. 57–58). Potreba po zavarovanju izhaja iz številnih nevarnosti raznih vrst in stopenj. Te nevarnosti ogrožajo premoženje, zdravje in življenje ljudi ter njihovo gospodarsko bit. Gospodarske posledice, ki nastanejo ob morebitnih uresničitvah nevarnosti, ovirajo delovanje posameznikov ter gospodarskih subjektov, zato je treba gospodarske posledice škodnih dogodkov, če jih ne moremo preprečiti, vsaj omiliti (Flis, 1999, str. 34). Z razvojem sodobnih tehnoloških rešitev, komunikacij, prometnih povezav ter globalizacije na vseh področjih se povečuje število možnih nevarnosti, ki bi utegnile ogroziti življenje ali premoženje posameznika in družbe (Žnidarič, 2004, str. 57). Zavarovalništvo ima torej pomembno vlogo pri zagotavljanju materialne dimenzije varnosti, saj zavarovalnica zagotavlja, da bo v primeru nastanka zavarovalnega primera, ki je vnaprej določen v zavarovalnih pogojih, izplačala dogovorjeno odškodnino (Žnidarič, 2004, str. 51).

Ker število možnih nevarnosti, ki nas ogrožajo, narašča, tudi zavarovalnice ponujajo vedno širši nabor zavarovalnih vrst. Mednje sodi tudi zavarovanje zlorab plačilnih kartic. Večina zavarovalnic v okviru tovrstnega zavarovanja ponuja naslednja kritja: zavarovanje tveganja zlorabe plačilne kartice; zavarovanje kraje ali ropa gotovine; zavarovanje za dodatne stroške in zavarovanje kraje ali izgube osebnih predmetov. Glede na to, da gre za nevarnost, kjer za finančne izgube ni odgovoren samo imetnik kartice, je smiselno najprej preveriti določanje odgovornosti za posamezno obliko zlorabe in opredeliti potek reklamacijskega postopka.

4.1 Odgovornost pri zlorabah plačilnih kartic

4.1.1 Odgovornost na strani izdajatelja

Obveznost za izdajatelja nastane takoj po tem, ko imetnik plačilnega instrumenta izdajatelja obvesti, da je prišlo do neodobrene plačilne transakcije oziroma da je plačilni instrument (kartica) izgubljen oziroma ukraden. Nastane tudi, ko je ponudnik plačilnih storitev odgovoren za neodobrene plačilne transakcije (ZPlaSS, 120. člen, 4. odstavek).

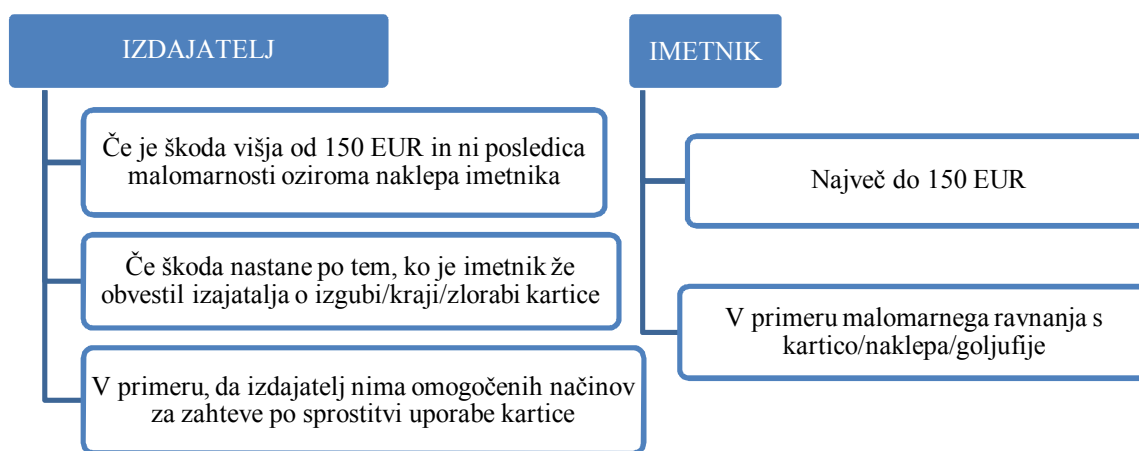
4.1.2 Odgovornost na strani imetnika

Do največ 150 EUR. Uporabnik plačilnega instrumenta krije izgubo zneska neodobrene plačilne transakcije do največ 150 EUR, če je izvršitev neodobrenih plačilnih transakcij, zaradi katerih je izguba nastala, posledica uporabe izgubljenega ali ukradenega plačilnega instrumenta ali plačilnega instrumenta, ki je bil zlorabljen, če uporabnik ni zavaroval osebnih varnostnih elementov plačilnega instrumenta. Če izguba presega 150 EUR, razliko krije izdajatelj plačilne kartice (ZPlaSS, 120. člen, 1. odstavek).

Za celotno izgubo. Če je izvršitev neodobrenih plačilnih transakcij posledica uporabnikove prevare ali če uporabnik naklepno ali pa zaradi hude malomarnosti ni izpolnil svojih obveznosti iz 116. člena ZPlaSS (120. člen, 2. odstavek). Poudariti je treba, da mora uporabnik kartice s to ravnati skrbno in brez odlašanja izdajatelja obvestiti o izgubi, kraji ali zlorabi plačilnega instrumenta (ZPlaSS, 116. člen).

Na Sliki 7 so prikazani možni scenariji odgovornosti v primeru zlorabe kartice, če gledamo z vidika, da sta vpletena samo imetnik ali izdajatelj.

Slika 7: Odgovornost za zlorabe plačilnih kartic po ZPlaSS



Vir: Povzeto in prirejeno po Zakonu o plačilnih storitvah in sistemih. Uradni list RS št. 58/09, 34/10, 9/11, 32/12 in 81/15.

4.1.3 Odgovornost za posamezno obliko zlorabe

Na izdajatelje plačilnih kartic sem naslovila vprašanje, kdo pri posamezni obliki zlorabe nosi odgovornost. Glede na to, da nisem prejela odgovora vseh vprašanih, podajam le prejete odgovore. Večina izdajateljev plačilnih kartic je mojemu vprašanju o odgovornosti pri posamezni obliki zlorabe v en glas pritrdilo, da je področje zelo kompleksno, z veliko možnimi scenariji, zato se ga ne da predstaviti v nekem okvirju, temveč je odvisno od primera do primera. Glede odgovornosti pri zlorabah sem prejela naslednje odgovore:

Zlorabe izgubljenih ali ukradenih kartic. Gorenjska banka, d.d.: »Takšna zloraba se lahko zgodi, še preden je imetnik preklical kartico, in še to le v primeru, da je imetnik imel zraven tudi PIN-številko (malomarno ravnanje). Do preklica kartice v tem primeru nosi škodno odgovornost imetnik kartice« (M. Rugelj, osebna komunikacija, 7. marca 2016). **Hranilnica Lon, d.d. (2016):** »Imetnik je odgovoren do škode v višini 150 EUR, ostalo krije hranilnica« (P. Ambrožič, osebna komunikacija, 7. marca 2016). **Nova KBM, d.d. (2016):** »Izid reklamacije ter škodna odgovornost sta odvisna od nekaj dejavnikov (čas blokade kartice, ravnanje s kartico, odvisno od primera do primera)« (T. Klinc, osebna komunikacija, 11. marca 2016). **Banka Koper, d.d. (2016):** »Vsak primer se obravnava individualno, zato ni možno vnaprej določiti, kdo in v kolikšni višini nosi odgovornost (T. Faust osebna komunikacija, 6. marca 2016).«

Zlorabe s ponarejenimi karticami. Vsi odgovori so bili enaki, to je, da škodno odgovornost nosi banka oziroma hranilnica (M. Rugelj, osebna komunikacija, 7. marca 2016; P. Ambrožič, osebna komunikacija, 7. marca 2016; T. Klinc, osebna komunikacija, 11. marca 2016; T. Faust, osebna komunikacija, 6. marca 2016).

CNP-zlorabe. Gorenjska banka, d.d. (2016): »V tem primeru gre za internetne transakcije in način kataloške prodaje. Do tega lahko pride, če prodajno mesto ne posluje v skladu z varnostnimi predpisi, ki omogočajo varno uporabo kartic. Zato je v takšnih primerih največkrat odgovornost na strani bank lastnic prodajnih mest (pridobitelj)« (M. Rugelj, osebna komunikacija, 7. marca 2016). **Hranilnica Lon, d.d. (2016):** »Če je transakcija opravljena v okviru 3-D Secure Code, je odgovornost na strani prodajnega mesta; če pa je transakcija opravljena na mestih, ki niso ustrezno zaščitena, pa je odgovoren imetnik sam« (P. Ambrožič, osebna komunikacija, 7. marca 2016). **Nova KBM, d.d. (2016):** »V primeru zlorabe, ko kartica ni fizično prisotna, se v večini primerov v reklamacijskem postopku štiti šibkejša stran – torej imetnik kartice« (T. Klinc, osebna komunikacija, 11. marca 2016). **Banka Koper, d.d. (2016):** »Škodna odgovornost se ugotavlja skladno z izidom 'chargeback' postopka« (T. Faust, osebna komunikacija, 6. marca 2016).

Zlorabe na bančnih avtomatih. Vsi odgovori so bili enaki, to je, da škodno odgovornost nosi banka oziroma hranilnica (M. Rugelj, osebna komunikacija, 7. marca 2016; P. Ambrožič, osebna komunikacija, 7. marca 2016; T. Klinc, osebna komunikacija, 11. marca 2016; T. Faust, osebna komunikacija, 6. marca 2016).

Kraja identitete. Gorenjska banka, d.d. (2016): Na banki pravijo, da tovrstnih primerov še niso imeli, vendar menijo, da škodno odgovornost v tem primeru nosi banka (M. Rugelj, osebna komunikacija, 7. marca 2016). **Hranilnica Lon, d.d. (2016):** »Škodno odgovornost nosi banka« (P. Ambrožič, osebna komunikacija, 7. marca 2016). **Nova KBM, d.d. (2016):** »Škodo krije banka« (T. Klinc, osebna komunikacija, 11. marca 2016). **Banka Koper, d.d. (2016):** »Vsak primer se obravnava individualno, zato ni možno vnaprej določiti, kdo in v kolikšni meri nosi odgovornost« (T. Faust, osebna komunikacija, 6. marca 2016).

4.1.4 Povračila za transakcije

V primeru, da imetnik kartice zaradi določenih odstopanj sproži reklamacijski postopek prek svojega izdajatelja kartice, ta pa naprej pri mednarodnem kartičnem sistemu (t. i. chargeback postopek) in izdajatelj ta postopek izgubi, je prodajno mesto dolžno banki nemudoma vrniti znesek reklamirane transakcije, skupaj s stroški postopka (Banka Koper, d.d., 2013). V primeru upravičene pritožbe tako izdajatelj kartice lahko povrne (zavrne) že nastalo transakcijo v korist imetnika kartice (angl. *chargeback*), (ZBS, 2011, str. 15).

(Nova KBM, d.d., T. Klinc, osebna komunikacija, 11. marca 2016) pojasnjuje, da imajo poslovanje s plačilnimi karticami in nadaljnje reklamacije vsaj dve strani:

- stran kartice (z njo upravlja izdajatelj kartice, ki lahko kartico spremlja ter nadzoruje porabo po njej v zvezi s podano reklamacijo, pritožbo, vprašanjem),
- stran dogodka transakcije (torej mesto, kjer imetnik s svojo kartico opravlja transakcijo in je pod okriljem pridobitelja (banko lastnico prodajnega mesta).

Imetnik kartice začne z reklamacijskim postopkom pri banki izdajateljici kartice. Banka izdajateljica v primeru reklamacije imetnika kartice sproži reklamacijski postopek pri banki lastnici prodajnega mesta prek svojih procesnih centrov. Postopek reklamacije prikazuje Slika 8.

Slika 8: Postopek reklamacije v primeru zlorabe plačilne kartice



Vir: Nova KBM, d.d., T. Klinc, osebna komunikacija, 11. marca 2016.

Vsi reklamacijski postopki se izvajajo na podlagi in v skladu s pravili MasterCard Worldwide Chargeback Guide ter Visa Europe Operating Regulations; pravila prav tako predpisujejo določene roke. V rednem reklamacijskem postopku MasterCard in Visa ne odločata o izidu transakcije, ampak banke, vpletene v spor, v skladu s prej omenjenimi pravili mednarodnih kartičnih sistemov. Če banke ne rešijo reklamacije v rednem reklamacijskem postopku, zadevo predajo v arbitražo. Kot arbiter v tem primeru nastopi MasterCard ali Visa. V primeru, da se v vmesnem času reševanja reklamacije prodajno mesto ter imetnik dogovorita o poravnavi oziroma rešitvi reklamacije, lahko prodajno mesto neposredno mimo reklamacije izvede storno reklamiranega zneska oziroma vračilo na kartico. V danem primeru mora imetnik obvestiti banko izdajateljico, da ta prekine postopek reklamacije, ki se že vodi v okviru mednarodnih kartičnih sistemov oziroma po njihovih veljavnih pravilih (T. Klinc, osebna komunikacija, 11. marca 2016).

Za zavarovanje morebitne škode, povezane z vračili reklamacijskih zahtevkov imetnikov kartic (*charge back* zahtevkov) in/ali s pogodbenimi kaznimi, ki bi jih banka morala plačati kartičnim sistemom, lahko banka kot varščino za transakcije v posameznem mesecu zadrži znesek do 5 % vseh plačil v mesecu, v katerem so bile transakcije opravljene. Banka znesek posamezne mesečne varščine vrne prodajnemu mestu po preteku reklamacijskega obdobja (Banka Koper, d.d., 2013). Prodajno mesto se za zagotavljanje varnosti pred *chargeback* zahtevki lahko zavaruje s t. i. *chargeback* zavarovanjem.

4.2 Bančno zavarovalništvo

Značilnost sodobnih finančnih trgov je prepletanje finančnih storitev kot tudi načinov njihove ponudbe. Za zelo uspešno in dinamično se je v zadnjih letih pokazala povezava bank in zavarovalnic. Bančno zavarovalništvo zajema vrsto oblik sodelovanja med banko in zavarovalnico. Najboljša opredelitev bančnega zavarovalništva je, da gre za ponudbo bančnih in zavarovalniških storitev prek skupnega prodajnega kanala in/ali isti skupini strank (Vičič, 2005). Kot navaja Munich Re (v Vičič, 2005, str. 60), so glavni razlogi za bančno zavarovalništvo v zavarovalnicah naslednji:

- poveča se baza potencialnih strank in s tem možnost dodatne prodaje storitev,

- povečana možnost priprave nove storitve. Širša baza potencialnih strank zavarovalnici omogoči ponudbo storitev, pri katerih bi brez povezave z banko težko dosegla želeno ekonomijo obsega in donosnost,
- boljše izkoriščanje ekonomije obsega, saj se lahko z vključitvijo bančno-zavarovalniških storitev znižajo fiksni stroški poslovanja, kar vodi v konkurenčno prednost, posledično pa lahko zavarovalnica ta vzvod izkoristi za ugodnejšo cenovno politiko.

4.3 Razvoj zavarovalniških produktov

Osnovni razvojni proces storitev v zavarovalnici mora omogočati, da bo nova storitev zavarovalnice oblikovana tako, da se bo prodajala, oblikovanje pa mora biti osredotočeno na področje, ki zagotavlja konkurenčno prednost, ki je vsebinske ter procesne narave. Vsebinska se nanaša na predmet zavarovanja ter kritja, procesna pa na povezavo s strankami in nov pristop pri uvajanju storitve na trg (Medveš, 2014, str. 62). Zavarovalni produkti se lahko pojavijo kot odgovor na ideje in razvoj konkurenčne zavarovalnice. Z njimi je mogoče povečati konkurenčno prednost zavarovalnice. Pomembna sta nenehen razvoj in iskanje novih možnosti – nov zavarovalni produkt ali večja dodana vrednost za zavarovance (Medveš, 2014).

Zavarovalnici razvoj novih zavarovalniških storitev omogoča osvajanje novih tržnih segmentov, večje zadovoljstvo obstoječih strank, širjenje ekonomske varnosti subjektov, večjo skladnost delovanja celotnega gospodarstva in učinkovitejše izvajanje procesov znotraj zavarovalnice (Vermeulen, 2004).

Pust (2009, str. 28) proces razvoja novega zavarovalnega produkta opredeljuje takole:

- **iskanje in zbiranje idej.** Pri razvoju novega zavarovalnega produkta sta najpomembnejša prava ideja in predlog o tem, kakšen naj bo zavarovalni produkt. Zavarovalnica mora definirati takšen produkt, ki ga trg potrebuje in pričakuje. Signal s trga: nov produkt zavarovalnice se večinoma porodi ob povpraševanju po nečem, kar zavarovalnica v določenem trenutku še ne nudi. To posledično predstavlja jasen signal za razvojni oddelek zavarovalnice, da je treba pripraviti nov produkt. Signal »od znotraj«: predlagatelji novega produkta se zelo pogosto pojavijo v zavarovalnici;
- **ocenjevanje in izbor idej.** Z različnimi tehnikami zavarovalnica določi, katera ideja je dobra, in zanjo poda vrednostno oceno ideje. Ocena ideje je produkt relativne pomembnosti posameznega dejavnika uspeha ideje in sposobnosti podjetja, da idejo uresniči;
- nadalje sledi **postopek razvijanja osnovnega koncepta** iz ideje, ki je bila glede na dejavnik uspeha najboljša. Šele na tej točki se prične dejanski razvoj novega zavarovalnega produkta. V to sodi priprava zavarovalnih pogojev in premijskih sistemov. Ustrezno zavarovalno kritje, ki ga nudi produkt, je zanimivo za trg, ravno

nasprotno pa je za zavarovalnico najbolj zanimiv produkt z ustreznimi nezavarovanimi nevarnostmi in izključitvami, kar posledično vodi v iskanje ustreznega kompromisa. Pri razvoju produkta običajno sodelujejo strokovnjaki z različnih področij dela, ki imajo zavarovalniške izkušnje iz sklepalnega in škodnega zavarovalnega posla;

- **poslovna analiza in izdelava aktuarskih izračunov.** Naloga aktuarjev je določiti premijo, ki bo naprej pokrila predvidene škode in stroške, hkrati pa mora biti konkurenčna;
- **dokončen razvoj koncepta** (vključno z IT-podporo) in testiranja;
- **uvajanje produkta na trg.**

Kot ugotavlja Potočnik (2004, str. 226), je razvoj novih produktov v zavarovalništvu odvisen predvsem od:

- zadostnega števila dobrih idej,
- potrebnih investicijskih sredstev in dobrih strokovnjakov,
- časa razvoja,
- stroškov razvoja,
- življenjskega cikla sedanjih storitev in
- potencialnega povpraševanja.

5 RAZISKOVALNI DEL

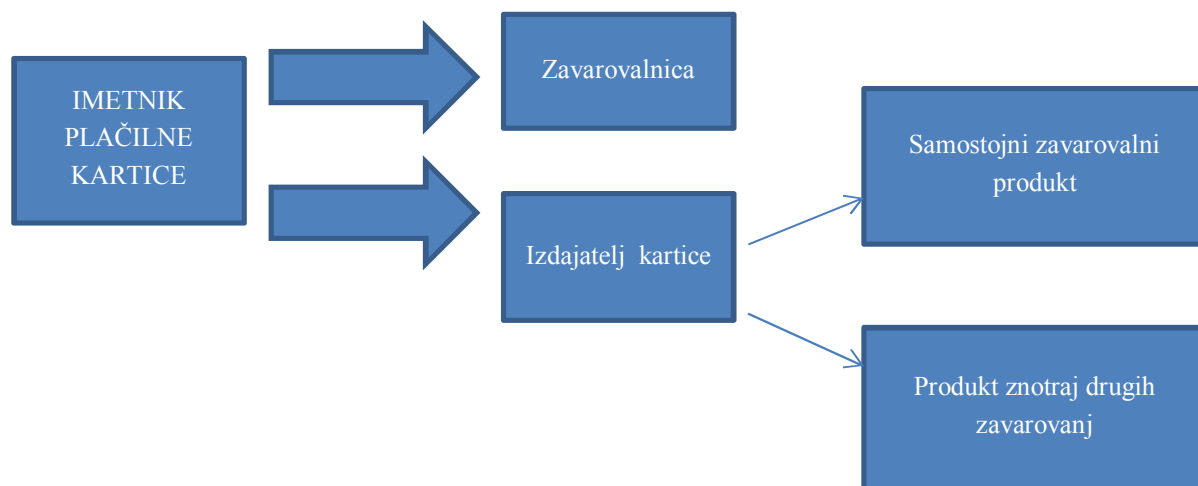
5.1 Prikaz možnosti zavarovanja plačilnih kartic v Sloveniji

Pred posledicami finančnih izgub v primeru zlorab plačilnih kartic nam številne banke kot posrednice pri trženju zavarovalnih produktov ponujajo zavarovanja plačilnih kartic. V magistrskem delu se osredotočam na zavarovanje, ki je na voljo posameznikom kot fizičnim osebam. Med pripravo gradiva za magistrsko delo sem naletela na vrsto zavarovanj, ki jih zavarovalnice nudijo pri zavarovanju plačilnih kartic, vendar se je treba omejiti. Prvič, zanimajo me posamezniki, osebne kartice in ne poslovne; drugič, zanima me tisto zavarovanje, ki je resnično vezano za zavarovanje zlorabe plačilne kartice, in ne druge vrste zavarovanj plačilnih kartic. Nekatere zavarovalnice ponujajo zavarovanje plačilnih kartic tudi znotraj zavarovanja premičnin kot dodatno kritje v nekaterih paketih. V okvir zavarovanja plačilnih kartic, ki je predmet proučevanja mojega dela, nikakor se smemo prištevati vseh vrst zavarovanj, ki so imetnikom ponujena oziroma so že vključena v naročnino kartic, saj vsa ne zajemajo tudi zavarovanja zlorabe. To so zavarovanja, kjer zavarovanje zlorabe plačilne kartice nikakor ni predmet zavarovanja, pa vendar se zavarovanje v večini primerov imenuje zavarovanje plačilnih kartic, znotraj tega pa se skriva npr. zavarovanje za primer brezposelnosti, trajne invalidnosti, nezgode in smrti. S sklenitvijo zavarovanja se lahko posameznik zavaruje do višine, do katere sam nosi

tveganje zlorabe (150 EUR), višjo škodo pa mora po zakonu poravnati banka (ZPlaSS, 120. člen).

Na Sliki 9 je grafični prikaz možnosti za sklepanje zavarovanja plačilnih kartic.

Slika 9: Možnosti, ki jih ima posameznik za sklepanje zavarovanja plačilnih kartic



Banke tržijo zavarovalne produkte za primer zlorabe plačilne kartice:

- kot samostojne produkte, ki jih stranka lahko sklene kot posameznik, proti doplačilu.
- znotraj kolektivnih zavarovanj, različnih asistenc, pri katerih je zavarovalec banka, stranka pa je zavarovanec. V primeru asistenc gre večinoma za zavarovanje kreditnih kartic z različnimi kritji, med katerimi so zlorabe kartic zgolj omenjene v primeru potovanja, cena pa je že vključena v mesečno oziroma letno nadomestilo za uporabo kartice.

V Tabeli 11 so prikazane posamične finančne institucije v Sloveniji in podatek o tem, ali ponujajo zavarovanje in če ga, na kakšen način ga ponujajo.

Tabela 11: Možnost zavarovanja zlorabe plačilne kartice posameznika po bankah oziroma hranilnicah v Sloveniji

Izdajatelj plačilne kartice	Samostojni produkt	Cena (v EUR na leto)	Produkt znotraj kolektivnega zavarovanja ali asistence
Abanka, d.d.	Da	9,9	Ne
Banka Koper, d.d.	Ne	/	Ne

se nadaljuje

Tabela 11: Možnost zavarovanja plačilne kartice posameznika po bankah oziroma hranilnicah v Sloveniji (nad.)

Izdajatelj plačilne kartice	Samostojni produkt	Cena (v EUR na leto)	Produkt znotraj kolektivnega zavarovanja ali asistenc
Banka Sparkasse, d.d.	Da	V nekatere bančne pakete je cena že vključena * dodatne storitve opcijsko	Da
Bks Bank AG, Bančna podružnica	Da	9	Ne
Deželna banka Slovenije, d.d.	Da	Ni podatka	Ni podatka
Gorenjska banka, d.d., Kranj	Da	9	Ne
Hranilnica Lon, d.d., Kranj	Ne (komitentom imajo v namenu produkt ponuditi še letos)	/	Ne
Hypo Alpe-Adria-Bank, d.d.	Da	9	Da
NKBM, d.d., Maribor	Da	7,33	Ne
NLB, d.d., Ljubljana	Da	Ni podatka	Ni podatka
Poštna banka Slovenije, d.d., Bančna skupina NKBM, d.d.	Da	7,33	Ne
Sberbank banka, d.d.	Ne	/	Ne
SKB banka, d.d., Ljubljana	Da	12	Ne

Legenda: * Izdajatelji, pri katerih podatkov o zavarovanju plačilnih kartic ni bilo mogoče najti na spletnih straneh in se prav tako niso odzvali na mojo prošnjo po posredovanju podatkov, so iz tabele izključeni. Ni podatka: na spletnih straneh so informacije o zavarovanju zlorab plačilnih kartic, vendar so pomanjkljive, na prošnjo po posredovanju podatkov pa nisem prejela odgovora.

Vir: Abanka, d.d., Zavarovanje kartic, 2016; Banka Koper, d.d., T. Faust, osebna komunikacija, 6. marca 2016; Banka Sparkasse, d.d., Udobni paketni računi, 2016; BKS bank AG bančna podružnica, B. Drganec, osebna komunikacija, 3. marca 2016; Deželna banka Slovenije, d.d., Premoženska zavarovanja, 2016; Gorenjska banka, d.d., Kranj, M. Rugelj, osebna komunikacija, 3. marca 2016; Hranilnica Lon, d.d., Kranj, P. Ambrožič, osebna komunikacija, 7. marca 2016; Hypo Alpe-Adria-Bank, d.d., Zavarovanje kartic in osebnih predmetov, 2016; Nova KBM, d.d., Zavarovanje za primer izgube ali kraje kartice, 2016; NLB, d.d., T. Šešič, osebna komunikacija, 18. decembra, 2015; Poštna banka Slovenije, d.d., M. Grahovec, osebna komunikacija, 3. marca 2016; Sberbank banka, d.d., I. Pašagić, osebna komunikacija, 3. marca 2016; SKB banka, d.d., Zavarovanje kartic plus, 2016.

Večina izdajateljev plačilnih kartic zavarovanja za primer zlorabe teh že ponuja. Nekateri zavarovanje ponujajo kot samostojen plačljiv produkt zavarovalnic, nekateri pa znotraj drugih zavarovanj, ki so bodisi plačljiva ali pa vključena v ceno članarine za uporabo kartice. Izdajatelji, ki so podali odgovor, da zavarovanja zaenkrat še ne ponujajo, so: Sberbanka, d.d., Banka Koper, d.d. ter Hranilnica Lon, d.d., kjer imajo sicer v načrtu, da bi

takšen produkt imetnikom plačilnih kartic ponudili še letos. Imetnik plačilne kartice za zavarovanje največ odšteje pri SKB banki, d.d., kjer letna premija za zavarovanje znaša 12 EUR, najmanj pa pri Novi KBM, d.d., oziroma Poštni banki Slovenije, d.d., kjer letna premija znaša 7,33 EUR.

5.2 Samostojni zavarovalni produkti zavarovalnic v Sloveniji

5.2.1 Zavarovalnica Triglav, d.d.

Za **Zavarovalnico Triglav, d.d.**, produkte tržijo naslednje banke: Abanka, d.d., BKS Bank AG, Bančna podružnica, Gorenjska banka, d.d., Kranj; Hypo Alpe-Adria-Bank, d.d., ter NLB, d.d., Ljubljana.

Zloraba. Za zlorabo kartice veljata plačilo blaga in storitev na prodajnem mestu in dvig gotovine v banki ali na bančnem avtomatu s strani tretje osebe z izgubljeno ali protipravno odvzeto kartico (Zavarovalnica Triglav, d.d., 2012).

Predmet zavarovanja (Zavarovalnica Triglav, d.d., 2012):

- zavarovanje krije škodo, ki jo zavarovanec utрпи zaradi zlorabe kartice s strani tretje osebe, ali drugo škodo, ki zavarovancu skladno s pogoji nastane ob škodnem dogodku;
- zavarovane so vse kartice, ki jih posamezna banka ali drug izdajatelj izda zavarovancu ali pooblaščenцу;
- kriti so škodni dogodki na območju Evrope, nastali zaradi protipravnega odvzema gotovine, osebnih predmetov ali mobilnega telefona, če so bili zavarovancu ti osebni predmeti vzeti skupaj s kartico. V primeru škode, nastale zaradi zlorabe kartice, pa kritje velja za škodne dogodke po vsem svetu.

Zavarovanje ne velja v primeru skimminga, vdora v informacijski sistem ter za zlorabe pri nakupih na daljavo (telefon, internet, pošta) (Zavarovalnica Triglav, d.d., 2012).

Natančnejši obseg kritja, ki ga Zavarovalnica Triglav, d.d., ponuja različnim bankam, je opredeljen v Tabeli 12.

Tabela 12: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Zavarovalnici Triglav, d.d.

Vrsta kritja	Vrsta limita	Višina limita Abanka, d.d. v EUR	Višina limita BKS bank AG, Gorenjska banka, d.d., HYPO ALPE ADRIA BANK, d.d. in NLB, d.d. v EUR
Zavarovanje tveganja zlorabe ukradenih ali izgubljenih plačilnih in kreditnih kartic			
Zloraba kartice s strani tretjih oseb	Limit po posamezni kartici po škodnem dogodku	150	150
	Limit za vse kartice za vse škodne dogodke na leto	2.000	1.000
Zavarovanje kraje ali ropa gotovine			
Protipravni odvzem gotovine	Limit za vse škodne dogodke na leto	200	200
Zavarovanje za dodatne stroške			
Stroški izdaje novih kartic	Limit po posamezni kartici po škodnem dogodku	10	10
	Limit za vse kartice za vse škodne dogodke na leto	50	50
Zavarovanje kraje ali izgube osebnih predmetov			
Stroški zamenjave ključev in ključavnic	Limit za vse škodne dogodke na leto	200	200
Stroški zamenjave osebnih dokumentov	Limit za vse škodne dogodke na leto	100	100
Stroški nakupa nove torbe ali denarnice	Limit za vse škodne dogodke na leto	150	100
Stroški klicev z mobilnega telefona	Limit za vse škodne dogodke na leto	150	100

Legenda: * Splošna višina limita, ki ga ponuja Zavarovalnica Triglav, d.d., je navedena v četrtem stolpcu Tabele 12. Za Abanko, d.d., so pri nekaterih vrstah kritja v pogodbi določene nekoliko drugačne višine limita.

Vir: Zavarovalnica Triglav, d.d., Zavarovanje zlorabe plačilnih kartic, 2016; Zavarovalnica Triglav, d.d., Posebni pogoji za zavarovanje zlorabe plačilnih kartic, 2012; Abanka d.d., Zavarovanje kartic, 2016.

Produkt Zavarovalnice Triglav, d.d., za zavarovanje zlorab plačilnih kartic je z vidika vrste kritja identičen med vsemi ponudniki (torej bankami), razlikuje se le pri višini limita pri nekaterih vrstah kritja. Če zavarovanje sklenemo prek Abanke, d.d., je denimo možno izplačilo za zlorabe kartic na letni ravni omejeno na največ 2.000 EUR. Če zavarovanje sklenemo pri ostali četverici bank, ki trži produkt Zavarovalnice Triglav, d.d., pa je najvišje izplačilo omejeno na 1.000 EUR. Prav tako je pri Abanki, d.d., višje izplačilo v

primeru stroškov za nakup nove torbe ali denarnice ter povrnitve stroškov klicev na mobilnem telefonu.

Zavarovalnica Triglav, d.d., je tudi edina izmed zavarovalnic v Sloveniji, kjer lahko posameznik zavarovanje sklene neposredno pri njih in ne samo prek izdajatelja plačilne kartice. Zavarovanje lahko neposredno sklenejo komitenti slovenskih bank, zavarovati je mogoče kartice samo ene banke ali več bank, premija pa znaša od 8 do 14 EUR letno – več v Tabeli 13 (Zavarovanje zlorabe plačilnih kartic, 2016).

Tabela 13: Višina letne premije ob neposredni sklenitvi zavarovanja pri Zavarovalnici Triglav, d.d.

	Kartice, izdane pri eni banki v EUR na leto	Kartice, izdane pri več bankah v EUR na leto
Vsa kritja (brez skimminga)	8	10
Vsa kritja z vključenim skimmingom	12	14

Legenda: * Seznam vseh kritij se nahaja v zgornji Tabeli 12.

Vir: Zavarovalnica Triglav, d.d., Zavarovanje zlorabe plačilnih kartic, 2016.

V primeru, da imetnik plačilne kartice zavarovanje neposredno sklene pri zavarovalnici, je kritje podano tudi za primer skimminga.

5.2.2 Zavarovalnica Tilia, d.d.

Za Zavarovalnico Tilio, d.d., trži produkt SKB banka, d.d.

Zloraba. Izraz zloraba pomeni nepooblaščen dvig gotovine v bankah ali na bančnih avtomatih z uporabo izgubljenih ali ukradenih kartic in plačila, izvršena v korist nepooblaščen osebe z uporabo izgubljenih ali ukradenih kartic (Zavarovalnica Tilia, d.d., 2014, str. 1).

Predmet zavarovanja (Zavarovalnica Tilia, d.d., 2014, str. 1):

- predmet zavarovanja je zloraba plačilnih in kreditnih kartic SKB banke,
- zavarovane so vse kartice, ki jih SKB banka, d.d. izda komitentu,
- po tem zavarovanju je krita škoda, ki nastane zaradi zlorabe izgubljenih, ukradenih kartic ter kraje ali ropa gotovine.

Zavarovalnica v primeru zlorabe plačilnih in kreditnih kartic krije škodo na območju celotnega sveta; medtem ko za druge vrste kritja izrecne omejitve niso posebej zapisane v pogojih (Zavarovalnica Tilia, d.d., 2014).

Višina limita pri Zavarovalnici Tilii, d.d., za zavarovanje zlorabe plačilne kartice je ločena glede na to, ali je kartica zlorabljen na bankomatu oziroma prek POS-terminala, medtem ko pri Zavarovalnici Triglav, d.d., tovrstnega razlikovanja ne opazimo. Pri določenih vrstah limita opazimo, da je možno izplačilo zavarovalnine največ trikrat letno, preostala proučevana zavarovatelja takšne omejitve ne pogojujeta. Več o obsegu krija, ki ga nudi Zavarovalnica Tilia, d.d., podajam v Tabeli 14.

Tabela 14: Obseg zavarovalnega krija za zavarovanje zlorabe plačilnih kartic pri Zavarovalnici Tilia, d.d.

Vrsta krija	Vrsta limita	Višina limita SKB, d.d. v EUR
Zavarovanje tveganja zlorabe ukradenih ali izgubljenih plačilnih in kreditnih kartic		
Zavarovanje zlorabe izgubljene ali ukradene kartice	Limit na izgubo in na leto za zlorabo/opravljen plačilo s kartico	3.000
	Limit po kartici in na leto za zlorabo z dvigom gotovine	250
Zavarovanje kraje ali ropa gotovine		
Zavarovanje predhodno dvignjene gotovine	Po dogodku in na leto	125
Zavarovanje za dodatne stroške		
Stroški prijave izgube/kraje kartice in izdaje nove kartice	Po dogodku, do 3-krat letno	12
Stroški identifikacijske kartice za uporabo spletne banke SKB NET	Po dogodku, do 3-krat letno	22
Zavarovanje kraje ali izgube osebnih predmetov		
Zavarovanje stroškov ponovne izdelave dokumentov	Po dogodku in na leto	100
Zavarovanje stroškov ponovne izdelave ključev	Po dogodku in na leto	300
Stroški nakupa nove torbe ali denarnice	Po dogodku in na leto	100
Stroški klicev z mobilnega telefona	Po dogodku in na leto	100

Vir: Zavarovalnica Tilia, d.d., Pogoji za zavarovanje zavarovalnega programa Zavarovanje kartic plus, 2014, str. 1-4.; SKB banka, d.d., Zavarovanje kartic plus, 2016.

5.2.3 Zavarovalnica Maribor, d.d.

Produkte za **Zavarovalnico Maribor, d.d.**, tržijo naslednje banke: Nova KBM, d.d., in Poštna banka Slovenije, d.d.

Zloraba. Izraz zloraba pomeni uporabo izgubljene ali ukradene kartice s strani nepooblaščen osebe (Zavarovalnica Maribor, d.d., 2010).

Predmet zavarovanja so (Zavarovalnica Maribor, d.d., 2010):

- zlorabe plačilnih ali kreditnih kartic ob izgubi ali kraji teh s strani nepooblaščen osebe;
- rop ali roparska tatvina (kadar je gotovina dvignjena s kartico);
- izguba ali kraja osebnih predmetov (če so izgubljeni/ukradeni skupaj s kartico);
- kriti so škodni dogodki na območju Evrope, nastali zaradi protipravnega odvzema gotovine, osebnih predmetov ali mobilnega telefona, če so bili zavarovancu ti osebni predmeti vzeti skupaj s kartico. V primeru škode, nastale zaradi zlorabe kartice, pa kritje velja za škodne dogodke po vsem svetu.

V splošnih pogojih je prav tako posebej navedeno, za katere zlorabe zavarovanje ne velja: skimming, skimming v POS-terminalu, zlorabe pri nakupih na daljavo (telefon, internet, pošta), vdor v informacijski sistem (npr. kraja identitete), postopek, ki se na prodajnem mestu ne izvaja pred očmi zavarovanca (Zavarovalnica Maribor, d.d., 2010).

Več o obsegu kritja, ki ga nudi Zavarovalnica Maribor, d.d., podajam v Tabeli 15.

Tabela 15: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Zavarovalnici Maribor, d.d.

Vrsta kritja	Vrsta limita	Višina limita v EUR
Zavarovanje tveganja zlorabe ukradenih ali izgubljenih plačilnih in kreditnih kartic		
Zavarovanje zlorabe izgubljene ali ukradene kartice	Limit po posamezni kartici po škodnem dogodku v primeru plačila preko POS s strani nepooblaščen osebe	2.000
	Limit za vse kartice na leto v primeru dviga gotovine s strani nepooblaščen osebe	150
Zavarovanje kraje ali ropa gotovine		
Zavarovanje predhodno dvignjene gotovine	Limit po škodnem dogodku in na leto	200
Zavarovanje za dodatne stroške		
Stroški prijave izgube/kraje kartice in izdaje nove kartice	Limit po posamezni kartici po škodnem dogodku	10
	Limit za vse kartice za vse škodne dogodke na leto	50
Zavarovanje kraje ali izgube osebnih predmetov		
Zavarovanje stroškov ponovne izdelave dokumentov	Po škodnem dogodku in na leto	100
Zavarovanje stroškov ponovne izdelave ključev	Po škodnem dogodku in na leto	300
Stroški nakupa nove torbe ali denarnice	Po škodnem dogodku in na leto	150
Stroški klicev z mobilnega telefona	Po škodnem dogodku in na leto	150

Vir: Zavarovalnica Maribor, d.d., Splošni pogoji za zavarovanje nevarnosti izgubljenih ali ukradenih plačilnih ali kreditnih kartic, 2010. Nova KBM, d.d., Zavarovanje kartic in osebnih predmetov, 2016.

Tudi pri Zavarovalnici Maribor, d.d., je vrsta limita ločena glede na to, ali je bila zloraba plačilne kartice izvedena prek POS-terminala ali bankomata. Višina limita se sicer nekoliko razlikuje, a posebnih odstopanj ne opazimo (več v primerjavi). Zavarovalnica Maribor, d.d., omejuje zgornjo mejo obveznosti zavarovalnice na leto pri 2.950 EUR (Zavarovanje kartic in osebnih predmetov, 2016).

5.2.4 Primerjava samostojnih zavarovalnih produktov zavarovalnic v Sloveniji

Primerjava zavarovalnih kritij nam razkriva podobnosti in razlike v ponudbah zavarovalnic oziroma bank na področju zavarovanja zlorab plačilnih kartic. Vse zavarovalnice ločijo zavarovanje kartic na: zavarovanje tveganja zlorabe izgubljene ali ukradene kartice, zavarovanje kraje ali ropa gotovine, zavarovanje za dodatne stroške ter zavarovanje kraje ali izgube osebnih predmetov. Vsem je skupno, da smo do zavarovanja dodatnih stroškov ter zavarovanja osebnih predmetov upravičeni le v primeru, da so ti ukradeni skupaj z zavarovano plačilno kartico. Skupna značilnost vseh samostojnih zavarovalnih produktov v Sloveniji je tudi, da noben ne nudi možnosti kritja v primeru CNP-zlorabe. Primerjava obsega kritja znotraj zavarovalnih produktov zavarovalnic v Sloveniji:

- **Zavarovanje tveganja zlorabe izgubljene ali ukradene kartice**

Pri analizi zavarovanja tveganja za zlorabo izgubljene ali ukradene kartice je treba opozoriti, da Zavarovalnica Triglav, d.d., ne loči zavarovanja zlorabe kartice glede na to, ali je bila zloraba storjena prek bankomata ali POS-terminala. Ostali dve proučevani zavarovalnici pa višino limita opredeljujeta za vsako zlorabo posebej. Prav iz tega razloga je skupna primerjava zavarovanja v grafikonu onemogočena, zato je iz tega izvzeta. Najvišji limit na leto in na zavarovalni primer, ki ga v primeru zlorabe plačilne kartice prek POS-terminala nudi Zavarovalnica Tilja, d.d., znaša 3.000 EUR, pri Zavarovalnici Maribor, d.d., pa je ta 2.000 EUR. V primeru zlorabe plačilne kartice na bankomatu znaša najvišji limit na leto in na zavarovalni primer pri Zavarovalnici Tilii, d.d. 250 EUR, pri Zavarovalnici Maribor, d.d., pa 150 EUR. Kot sem že omenila, Zavarovalnica Triglav, d.d., ne loči zlorabe glede na to, ali je bila ta izvedena prek POS-terminala oziroma prek bankomata. Najvišji limit po posamezni kartici po škodnem dogodku znaša 150 EUR, limit za vse kartice in vse škodne dogodke na leto pa je 1.000 EUR.

- **Zavarovanje kraje ali ropa gotovine**

V primeru napada ali kraje gotovine po dvigu na bankomatu smo najbolj zaščiteni pri Zavarovalnici Triglav, d.d., ter Zavarovalnici Maribor, d.d. (200 EUR), najmanj pa pri Zavarovalnici Tilii, d.d. (125 EUR).

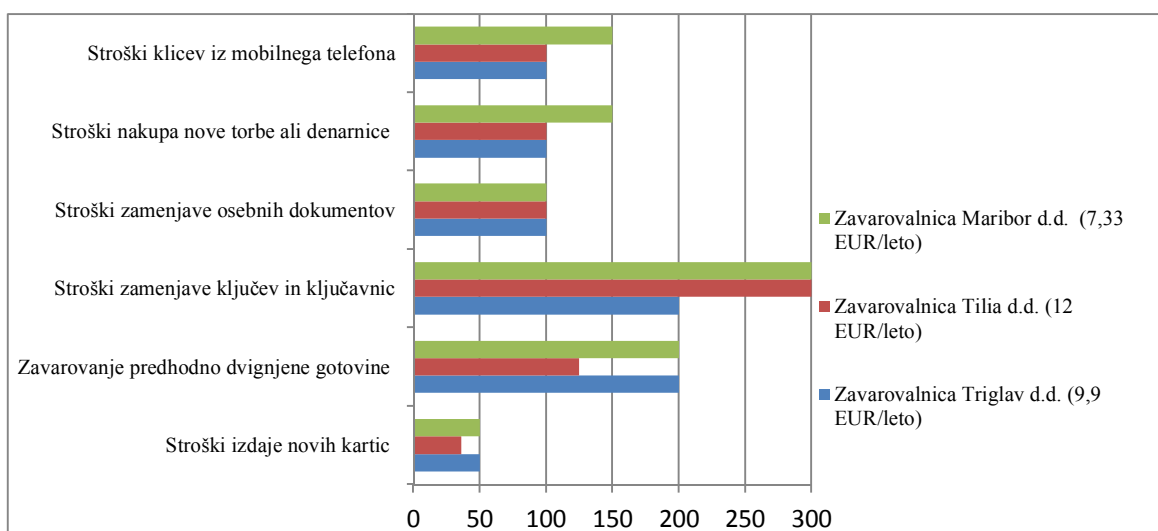
- **Zavarovanje za dodatne stroške**

Zavarovanje dodatnih stroškov zajema stroške preklica in izdaje novih kartic, Zavarovalnica Tilia, d.d., pa komitentom SKB banke, d.d., nudi tudi nadomestilo za stroške, ki nastanejo v primeru odtujitve identifikacijske kartice za uporabo njihove spletne banke. Limit za stroške izdaje nove kartice za posamičen škodni dogodek znaša pri Zavarovalnici Triglav, d.d., ter pri Zavarovalnici Maribor, d.d., 10 EUR, limit za vse kartice in vse škodne dogodke na leto pa pri omenjenih zavarovalnicah znaša 50 EUR. Zavarovalnica Tilia, d.d., za posamičen škodni dogodek nudi 12 EUR, letni limit pa je omejen do največ 3-krat letno.

- **Zavarovanje kraje ali izgube osebnih predmetov**

V primeru stroškov za zamenjavo ključev in ključavnic najvišjo zavarovalnino izplačata Zavarovalnica Maribor, d.d., in Zavarovalnica Tilia, d.d. (300 EUR), najnižjo pa Zavarovalnica Triglav, d.d. (200 EUR). Za stroške nakupa nove torbe oziroma denarnice smo do najvišje zavarovalnine upravičeni pri Zavarovalnici Maribor, d.d. (150 EUR), pri ostalih dveh proučevanih zavarovalnicah pa je višina limita enaka in znaša 100 EUR. V primeru kraje mobilnega telefona ter s tem povezanih stroškov nam bo Zavarovalnica Maribor, d.d., izplačala 150 EUR, preostali zavarovalnici pa 100 EUR. Limit za stroške izdelave osebnih dokumentov je pri vseh treh proučevanih zavarovalnicah enak in znaša 100 EUR.

Slika 10: Primerjava zavarovalnih kritij za zavarovanje zlorabe plačilnih kartic pri slovenskih zavarovalnicah



Legenda: * V grafikonu zaradi neenotne delitve ni mogoča primerjava zavarovalnega kritja za primer izgube ali kraje kartice, zato je primerjava opisana zgoraj.

Vir: Zavarovalnica Maribor, d.d., Splošni pogoji za zavarovanje nevarnosti izgubljenih ali ukradenih plačilnih ali kreditnih kartic, 2010; Zavarovalnica Tilia, d.d., Pogoji za zavarovanje zavarovalnega programa Zavarovanje kartic plus, 2014, str. 1-4; Zavarovalnica Triglav, d.d., Zavarovanje zlorabe plačilnih kartic, 2016.

5.3 Zavarovanje plačilnih kartic znotraj drugih produktov v sklopu kolektivnega zavarovanja imetnikov plačilnih kartic

Večina bank svojim imetnikom plačilnih kartic (predvsem kreditnih) zagotavlja tudi različna zavarovanja, katerih cena je že vključena v letno članarino. V večini primerov je vključeno le nezgodno zavarovanje oziroma zavarovanje invalidnosti, nekatere banke pa ponujajo pakete, ki vključujejo tudi zavarovanje zlorab plačilnih kartic.

5.3.1 Hypo Alpe-Adria-Bank, d.d.

Hypo Alpe-Adria-Bank, d.d., svojim komitentom za kreditne kartice nudi kolektivno zavarovanje v okviru Hypo bančnih paketov z maksimalnim zavarovanjem v sklopu ERGO zavarovalnice (več v Tabeli 16).

Tabela 16: Vrsta in višina zavarovalnih kritij za zavarovanje zlorabe kartic po posamičnih paketih HYPO Alpe Adria Bank, d.d.

Vrsta kritja	Višina limita Paket plus v EUR	Višina limita Paket E v EUR	Višina limita Paket Top, Exclusive, Top Depozitni v EUR
Protipravni odvzem gotovine pri bankomatu	200	300	500
Zloraba kartice	700	1.000	2.000
Nadomestilo za odtujene ključe in dokumente	200	300	500
Pravna pomoč	50	100	150

Vir: Hypo Alpe-Adria-Bank, d.d., Seznam zavarovalniških storitev v bančnih paketih, 2016.

Višina limita za posamezno vrsto kritja je odvisna od izbire bančnega paketa. Vsi paketi vključujejo zavarovanje zlorabe plačilne kartice, zavarovanje predhodno dvignjene gotovine, nadomestilo za izgubljene ključe in dokumente. Poleg tega paketi nudijo tudi pravno pomoč, česar pri individualnih policah za zavarovanje plačilnih kartic še nismo opazili. Zavarovalnica povrne škodo zaradi protipravno odvzete gotovine v primeru, da je zavarovanec dvignil gotovino na bankomatu in je prišlo do protipravnega odvzema gotovine v času dveh ur po opravljenem dvigu, ter v primeru, da je zavarovanec dvig gotovine na bankomatu moral izvesti zaradi resne grožnje s strani tretje osebe (SP-ERG_ZIK/2, 19. člen). Zavarovanje kritje škodo v primeru opravljenih nepooblaščenih transakcij, ki bremenijo zavarovančev račun, če je do zlorabe prišlo v 24 urah pred trenutkom, ko je zavarovanec izgubo ali odtujitev plačilne kartice prijavil zavarovalcu (banki) (SP-ERG_ZIK/2, 19. člen).

5.3.2 Raiffeisen banka, d.d.

Raiffeisen banka, d.d., ima z zavarovalnico Uniqa Versicherungen AG sklenjeno skupinsko zavarovalno polico v korist uporabnikov kreditno-plačilnih kartic. Zavarovanci po tej polici so vsi imetniki kreditno-plačilnih kartic, ki jih izdaja omenjena banka. Podatkov za višino limita in za posamezno vrsto kritja žal ni bilo moč pridobiti.

Zavarovanje krije (Uniqa Versicherungen AG, 2012):

- zavarovanje zlorabe izgubljene ali ukradene kartice, skimming,
- povrnitev stroškov za zamenjavo uradnih osebnih dokumentov in ključev, izgubljenih ali ukradenih skupaj s kartico.

Zavarovalno kritje velja za transakcije, kjer ni potrebna fizična prisotnost kartice za nedovoljene posle do 45 dni pred datumom vložitve zahtevka za blokado kartice. Zavarovalno kritje velja za transakcije, ki vključujejo fizično prisotnost kartice za nedovoljene transakcije do 48 ur pred vložitvijo zahtevka za blokado kartice. Uniqa Versicherungen AG. je tako med proučevanimi edina zavarovalnica, ki v Sloveniji nudi kritje tudi za primer skimminga ter za CNP-zlorabe.

5.3.3 Kartice Diners

Diners Club Slovenija, d.o.o., ima pri Generali zavarovalnici, d.d. Ljubljana, sklenjeno zavarovanje za imetnike plačilnih kartic. Generali zavarovalnica, d.d. Ljubljana, imetnikom Diners kartice nudi vse vrste kritja, ki jih druge zavarovalnice ponujajo bankam, da jih te tržijo kot samostojne produkte, pogrešamo le zavarovanje dodatnih stroškov (zamenjava in preklic kartice).

Najvišji limit na leto in na zavarovalni primer, ki ga v primeru zlorabe plačilne kartice prek POS nudi zavarovalnica, znaša 3.000 EUR, v primeru zlorabe na bančnem avtomatu pa je najvišji limit 250 EUR. Odškodnina v primeru kraje ali ropa predhodno dvignjene gotovine je omejena na 125 EUR. Natančna opredelitev zavarovanja za krajo ali izgubo osebnih predmetov je opredeljena v Tabeli 17.

Tabela 17: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Generali zavarovalnici, d.d. Ljubljana

Vrsta kritja	Vrsta limita	Višina limita v EUR
Zavarovanje tveganja zlorabe ukradenih ali izgubljenih plačilnih in kreditnih kartic		
Zavarovanje zlorabe izgubljene ali ukradene kartice	Limit po dogodku in na leto v primeru izvršenega plačila s strani nepooblaščenih oseb	3.000

se nadaljuje

Tabela 17: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Generali zavarovalnici, d.d. Ljubljana (nad.)

Vrsta kritja	Vrsta limita	Višina limita v EUR
Zavarovanje zlorabe izgubljene ali ukradene kartice	Limit po kartici in na leto v primeru dviga gotovine s strani nepooblaščenih oseb	250
Zavarovanje kraje ali ropa gotovine		
Zavarovanje predhodno dvignjene gotovine	Po dogodku in na leto	125
Zavarovanje kraje ali izgube osebnih predmetov		
Zavarovanje stroškov ponovne izdelave dokumentov	Po dogodku in na leto	100
Zavarovanje stroškov ponovne izdelave ključev ali zamenjave ključavnic	Po dogodku in na leto	300
Stroški nakupa nove torbe ali denarnice	Po dogodku in na leto	100
Stroški klicev z mobilnega telefona	Po škodnem in na leto	100

Vir: Generali Zavarovalnica, d.d. Ljubljana, Splošni pogoji za zavarovanje imetnikov kartice Diners Club, 2010.

5.4 Zavarovalni produkti v tujini

Izbor zavarovalnic za primerjavo ni bil ravno enostaven, saj je podatke izjemno težko pridobiti ali pa so pomanjkljivi. Izmed vseh proučevanih zavarovalnih produktov sem izbrala nekaj najbolj zanimivih primerov, ki mi bodo služili kot podlaga za sestavo najbolj zanimivega zavarovalnega produkta za področje zavarovanja plačilnih kartic.

5.4.1 American Express za področje ZDA

Pri zavarovanju, ki ga imetnikom ponuja American Express Company, ugotavljamo, da pokriva tudi vrsto kritja, ki ga pri analizi zavarovanja zlorab plačilnih kartic v Sloveniji nismo opazili, to je krajo identitete. Letno nadomestilo za zavarovanje znaša 39,99 ameriških dolarjev.

Zavarovanje krije (Lost wallet protector, 2016).

- zavarovanje ponarejenih kreditnih kartic (višina limita znaša 5.000 ameriških dolarjev),
- krajo identitete (višina limita znaša 1.000 ameriških dolarjev),
- pomoč pri izgubi/kraji mobilnega telefona ter asistenca pri izgubi potnega lista ali voznškega dovoljenja.

5.4.2 Citibank Czech Republic, a.s.

Citibank CZ, a.s., ima zavarovanje zlorabe plačilnih kartic urejeno prek zavarovalnice BNP Paribas Cardif Pojištevna, a.s. Zavarovanje je namenjeno uporabnikom Citi Credit Card Gold ter Gold Citi Card Debit Card, strošek zavarovanja pa je že vključen v ceno letne članarine. Zavarovanci imajo pravico do zavarovalnine v primeru zlorabe izgubljene oziroma ukradene kartice, če kartica ni bila zlorabljen več kot 72 ur, preden je imetnik zlorabo prijavil banki in zahteval blokado kartice (Citibank CZ, 2016). Več o zavarovalnem kritju je podano v Tabeli 18.

Tabela 18: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Citibank CZ, a.s. (produkt: Fraudulent usage 50)

Vrsta kritja	Vrsta limita	Višina limita v EUR
Zavarovanje zlorabe izgubljene ali ukradene kartice	Največ 3-krat v koledarskem letu	150
Neavtorizirana transakcija z uporabo PIN-kode	Največ 3-krat v koledarskem letu	1.850
Stroški za zamenjavo ključev	Največ 3-krat v koledarskem letu	110
Stroški za menjavo osebnih dokumentov	Največ 3-krat v koledarskem letu	110

Legenda: * Višina limita, preračunana in zaokrožena iz čeških kron v EUR po menjalnem tečaju Banke Slovenije dne 12. 3. 2016

Vir: Citibank Czech Republic, a.s., Fraudulent usage Insurance 50, 2016.

5.4.3 Komerčni banka, a.s.

Komerčni banka, a.s., ponuja podobno vrsto kritja kakor zavarovalnice v Sloveniji, podoben je tudi strošek letnega nadomestila. Opazimo le nekatere razlike pri višini limita, pogrešamo pa zavarovanje stroškov za preklic in menjavo kartice. Podrobnejši opis kritja je opredeljen v Tabeli 19.

Tabela 19: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Komerčni banki, a.s. (produkt: Insurance against misuse of a card)

Vrsta kritja	Višina limita v EUR
Zavarovanje tveganja zlorabe ukradenih ali izgubljenih plačilnih in kreditnih kartic	
Zloraba plačilne kartice – POS	740
Zloraba plačilne kartice – bankomat	370
Zavarovanje kraje ali ropa gotovine	
Zavarovanje predhodno dvignjene gotovine	185

se nadaljuje

Tabela 19: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Komerčni banki, a.s. (produkt: Insurance against misuse of a card) (nad.)

Vrsta kritja	Višina limita v EUR
Zavarovanje kraje ali izgube osebnih predmetov	
Zavarovanje zlorabe ukradenega telefona	110
Stroški menjave ukradenega telefona	110
Stroški zamenjave ključev	110
Stroški zamenjave os. dokumentov	18
Letno nadomestilo	10,5

Legenda: * Višina limita, preračunana in zaokrožena iz čeških kron v EUR po menjalnem tečaju Banke Slovenije dne 12. 3. 2016

Vir: Komerčni banka, a.s, Insurance against misuse of a card, 2016.

5.4.4 Sberbank CZ, a.s.

Pregled vrste kritja pri Sberbanki CZ, a.s., je zanimiv, ker zavarovanje zlorabe plačilne kartice obsega tudi brezstične kartice in CNP-zlorabe. Imetnikom prav tako dokaj visoko višino limita zavarovanja ponuja v primeru fizičnega nasilja pri bankomatu. Banka ponuja produkt zavarovalnice BNP Paribas Cardif Pojiščovna, a.s. Zanimiva je tudi dodatna ponudba zavarovanja kraje ali izgube osebnih predmetov, saj opazimo tudi nekatere vrste kritij, ki jih med dosedanja analizo še nismo zaznali. To so: zavarovanje kraje oziroma izgube očal, multimedijskih predvajalnikov, prenosnih računalnikov, fotoaparatorov in mobilnih naprav. Širok nabor različnih kritij pa je verjetno tudi razlog za nekoliko višjo ceno zavarovanja, saj ta na letni ravni znaša 26,16 EUR. Stroški za blokado ter izdajo nove kartice so vključeni v višini odškodnine v primeru zlorabe plačilne kartice. Podrobnejši obseg kritja se nahaja v Tabeli 20.

Tabela 20: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Sberbank CZ, a.s. (produkt: Fraud Insurance for Payment Cards)

Vrsta kritja	Vrsta limita	Višina limita v EUR
Zavarovanje tveganja zlorabe ukradenih ali izgubljenih plačilnih in kreditnih kartic		
Obdobje zavarovanja: 96 ur pred poročilom o kraji/izgubi kartice		
Zloraba plačilne kartice (vključuje brezstične transakcije in transakcije na internetu)	Limit po škodnem dogodku (največ 3-krat letno)	150
Zloraba plačilne kartice – z uporabo PIN številke	Limit po škodnem dogodku (največ 3-krat letno)	1.850
Zavarovanje kraje ali ropa gotovine		
Zavarovanje predhodno dvignjene (v roku 48 ur po dvigu)	Limit po škodnem dogodku	75
	Limit na leto	220
Zavarovanje gotovine v primeru grožnje oziroma fizičnega nasilja pri bankomatu	Limit po škodnem dogodku	370
	Limit na leto	1.110

se nadaljuje

Tabela 20: Obseg zavarovalnega kritja za zavarovanje zlorabe plačilnih kartic pri Sberbank CZ, a.s. (produkt: Fraud Insurance for Payment Cards) (nad.)

Vrsta kritja	Vrsta limita	Višina limita v EUR
Zavarovanje kraje ali izgube osebnih predmetov		
Ključ		
Osebni dokumenti		
Denarnica, torbica		
Očala		
MP3/MP4, fotoaparat		
Prenosni računalnik		
Mobilne naprave		
Obdobje zavarovanja za stroške z mobilnim telefonom:	Limit po škodnem dogodku	740
24 ur pred poročilom o kraji/izgubi	Limit na leto	2.960
Mesečno nadomestilo		2,18

Legenda: * Višina limita, preračunana in zaokrožena iz čeških kron v EUR po menjalnem tečaju Banke Slovenije dne 12. 3. 2016.

Vir: Sberbank CZ, a.s., Fraud Insurance for Payment Cards, 2016.

5.4.5 UniCredit Bank Czech Republic & Slovakia, a.s.

Zavarovanje velja tako za transakcije, kjer mora biti kartica fizično prisotna, kakor za CNP-transakcije. Opažamo, da zavarovatelj Generali, nudi tudi zavarovanje dodatnih stroškov, ki smo jih opazili le pri Sberbanki CZ, a.s., to so: stroški menjave ukradenega telefona, stroški menjave ukradenih korekcijskih očal in multimedijskih predvajalnikov. Podatka o strošku zavarovanja ni bilo mogoče pridobiti. Tabela 21 prikazuje obseg zavarovalnega kritja v okviru SAFE BASIC.

Tabela 21: Obseg zavarovalnega kritja SAFE BASIC za zavarovanje zlorabe plačilnih kartic pri UniCredit Bank Czech Republic & Slovakia, a.s. (produkt: Insurance against card misuse)

Najvišji limit	1.100 EUR	
Obdobje zavarovanja	120 ur pred poročilom o kraji/zlorabi kartice	
Osnovno zavarovanje vključuje	Finančna izguba zaradi zlorabe izgubljene/ukradene kartice	
	Stroški za ponovno izdelavo dokumentov	
	Stroški za ponovno izdajo kartice	
	Stroški za ponovne izdelave ključev	
	Zavarovanje predhodno dvignjene gotovine	
Dodatno zavarovanje vključuje	Stroški menjave ukradenega mobilnega telefona	185 EUR
	Zavarovanje zlorabe ukradenega mobilnega telefona	
	Stroški za nakup nove denarnice	110 EUR

Legenda: * Višina limita, preračunana in zaokrožena iz čeških kron v EUR po menjalnem tečaju Banke Slovenije dne 12. 3. 2016.

Vir: UniCredit Bank Czech Republic and Slovakia, a.s., Insurance against card misuse, 2015.

Tabela 22: Obseg zavarovalnega kritja SAFE PLUS za zavarovanje zlorabe plačilnih kartic pri UniCredit Bank Czech Republic & Slovakia, a.s. (produkt: Insurance against card misuse)

Najvišji limit	1.850 EUR	
Obdobje zavarovanja	120 ur pred poročilom o kraji/zlorabi kartice	
Osnovno zavarovanje vključuje	Finančna izguba zaradi zlorabe izgubljene/ukradene kartice	
	Stroški za ponovno izdelavo dokumentov	
	Stroški za ponovno izdajo kartice	
	Stroški za ponovne izdelave ključev	
	Zavarovanje predhodno dvignjene gotovine	
Dodatno zavarovanje vključuje	Stroški menjave ukradenega mobilnega telefona	370 EUR
	Zavarovanje zlorabe ukradenega mobilnega telefona	
	Stroški menjave ukradenih multimedia predvajalnikov	185 EUR
	Stroški menjave ukradenih korekcijskih očal	185 EUR
	Stroški za nakup nove denarnice	110 EUR

Legenda: * Višina limita, preračunana in zaokrožena iz čeških kron v EUR po menjalnem tečaju Banke Slovenije dne 12. 3. 2016.

Vir: UniCredit Bank Czech Republic and Slovakia, a.s., Insurance against card misuse, 2015.

5.5 Pomanjkljivosti zavarovanja

Zavarovanje naj bi imetnike plačilnih kartic varovalo pred finančnimi izgubami v primeru zlorabe izgubljene oziroma ukradene kartice. S pomočjo analize produktov različnih zavarovalnic za primer zlorabe plačilnih kartic ugotavljam, da so si produkti med seboj po vrstah kritja sicer podobni, a znotraj ponudbe po posamičnem kritju precej različni. Vsem je skupno to, da je zavarovanje zlorabe kartice le del zavarovanja, vsa ostala kritja pa so povezana s preostalimi stroški, ki nam nastanejo v primeru kraje/izgube plačilne kartice skupaj z drugimi predmeti. To izhaja tudi iz dejstva, da običajni imetnik plačilne kartice niti ne pozna svojih zakonskih pravic v primeru zlorabe, ne zaveda se torej, da nosi delež odgovornosti za zlorabo le v omejenih okoliščinah. V Sloveniji žrtev zlorabe plačilne kartice nosi odgovornost največ do 150 EUR, zato tudi oglaševanje oziroma ponudba višjega kritja za primer zlorabe plačilne kartice ni primerna. Takšna ponudba je pravzaprav zavajajoča, ker imetnik kritja, ki je višje od 150 EUR, ne potrebuje, saj je v tem primeru po zakonu dolžan odgovornost prevzeti izdajatelj kartice. Nekateri avtorji celo menijo, da je zavarovanje večinoma nepotrebno in goljufivo, saj mora izdajatelj to zaščito že po zakonu ponuditi kot samoumevno, ne pa proti doplačilu.

Credit Consulling Society imetnikom plačilnih kartic svetuje, da se v primeru, ko želijo skleniti tovrstno zavarovanje, najprej prepričajo naslednje (Do you need credit card loss insurance or another credit card scam, 2016):

- imetnik se mora najprej soočiti s pravicami, ki jih je izdajatelj po zakonu dolžan spoštovati (po našem zakonu – ZPlaSS, je imetnik odgovoren maksimalno do 150 EUR);
- pregledati mora, pri katerih karticah je zavarovanje že vključeno v članarino. Npr. Visa in MasterCard imata politiko ničelne odgovornosti, kar pomeni, da v primeru, ko uporabnik sporoči zlorabo/izgubo kartice, ta ni odgovoren za neodobrene transakcije v primeru skrbne rabe kartice;
- veliko zavarovalnic, ki ponujajo zavarovanje plačilnih kartic, imetnikom obljublja povrnitev vseh stroškov v primeru zlorabe, s tem da imetnike ustrahujejo, da bodo v primeru zlorabe in brez tovrstnega zavarovanja sami nosili celotne stroške, ki bi jih povzročila zloraba.

Glede zavajajoče ponudbe zavarovanja plačilnih kartic zasledimo zanimiv primer iz Velike Britanije, kjer je Financial Conduct Authority v letu 2015 objavil seznam bank, ki so ponujale goljufivo zavarovanje znotraj različnih produktov (Card security product holders: claim compensation by 18 March 2016, 2016). Imetnikom plačilnih kartic je bilo ponujeno zavarovanje, ki je obsegalo večje kritje od imetnikove škodne odgovornosti. Kritje je tako obsegalo tudi primer zlorabe, ko imetnik nikakor ni več odgovoren, to je za zlorabe po podanem poročilu o izgubi/odtuitvi kartice, pred poročanjem o zlorabi pa je imetnik konkretno v Veliki Britaniji odgovoren do največ 50 funtov. Banke so krivdo priznale, zato so morale vsem, ki so pristali na sklenitev zavarovanja, ponuditi nadomestilo za že vplačano zavarovanje od leta 2005 naprej. Za povrnitev stroškov je bilo tako vpoklicanih skoraj 2 milijona imetnikov plačilnih kartic, ki so sklenili omenjeno zavarovanje. Banke, ki so ponujale goljufive produkte, so: AIB Group, Barclays Bank Plc, Capital One, Clydesdale Bank PLC, HSBC Bank plc, Lloyds Bank plc, Northern Bank, Santander UK plc, Tesco Personal Finance, The Co-operative Bank plc in The Royal Bank of Scotland plc.

5.6 Priložnosti za uvedbo novega produkta na trg

Tržno okolje se nenehno spreminja, kot posledica tega pa nastaja veliko novih nevarnosti. Zavarovalnica to pojmuje kot nove priložnosti za uspešno prilagajanje razmeram na trgu. Zavarovalnice so z tehnološkim napredkom soočene z velikimi izzivi določanja novih nevarnosti. Prav tehnološki napredek predstavlja tudi nove nevarnosti za zlorabe plačilnih kartic. Zavarovalnica se mora prilagoditi potrebam in povpraševanju, ki izhajajo tudi iz zavedanja nevarnosti, ki grozijo imetnikom plačilnih kartic. Ker ljudje želijo ohranjati raven svoje varnosti tudi na področju nastajajočih novih nevarnosti, je jasno, da se bodo

zavarovali tudi pred novimi tveganji. Zavarovalnica je tista, ki mora zavarovalni produkt, ki pokriva nove nevarnosti, ponuditi čimprej, saj jo bo sicer prehitela konkurenca.

Izhajajoč iz dejstva, da je v fazi razvoja novega zavarovalnega produkta najpomembnejša prava ideja oziroma predlogi o tem, kakšen bo naj novi zavarovalni produkt, zavarovalnici predlagam postavitev kritij za naslednje nevarnosti:

- **zagotovitev kritja za CNP-transakcije**, saj tovrstnega kritja v Sloveniji ne ponuja še nobena zavarovalnica. Dober zgled za primer kritja tovrstnih zlorab opazimo pri Unicredit banki na Češkem in Slovaškem ter pri Sberbanki na Češkem, ki tržijo produkte različnih zavarovateljev. Glede na to, da večina imetnikov svoje plačilne kartice pogosto uporablja za oddaljene nakupe, je zaščita CNP nujno potrebna, saj bi v imetniku povzročila potrebo po tovrstnem zavarovanju, ker se zaveda pogostosti uporabe plačilne kartice na spletu;
- **zagotovitev kritja za brezstične transakcije**, ki ravno tako še ni v ponudbi zavarovalnic v Sloveniji, zasledili pa smo jo pri Sberbanki na Češkem. Brezstične transakcije omogočajo izvedbo transakcije brez avtorizacije, limit porabe brez številke PIN pa je omejen za nakup do 15 EUR, največ štirikrat v posameznem dnevu. V času raziskave je bilo izdajateljem plačilnih kartic posredovano tudi vprašanje o možnosti povišanja limita za nakup brez avtorizacije. Vsi vprašani izdajatelji plačilnih kartic, ki so podali odgovore, trdijo, da limita ni mogoče povišati. Pri tovrstnih transakcijah velja enako pravilo odgovornosti v primeru zlorabe kot pri običajnih plačilnih karticah, kjer imetnik nosi škodno odgovornost največ do začetnih 150 EUR izgube. V Sloveniji sicer vsi izdajatelji trenutno še ne omogočajo brezstičnega plačevanja, vendar ga v prihodnosti bodo, zato je prav prilagoditev zavarovalnice na takšno obliko nevarnosti bistvenega pomena, da bo pripravljena na vstop novih izdajateljev na trg brezstičnih kartic in takojšnjo ponudbo zavarovanja;
- **zaščita v primeru fizičnega napada pri bankomatu**. Glede na to, da smo pri zavarovateljih v Sloveniji opazili predvsem kritje nevarnosti kraje gotovine po dvigu z bankomata, v tujini pa tudi kritje nevarnosti fizične prisile dviga gotovine, bi bilo smotno, da zavarovalnice razmislijo o ponudbi takšnega kritja. Npr. Sberbanka na Češkem ima v ponudi dokaj visok limit za zavarovanje gotovine v primeru fizičnega napada pri bankomatu, poleg tega pa tudi daljše obdobje zavarovanja v primeru kraje/izgube dvignjene gotovine. Pri zavarovateljih v Sloveniji pa je doba zavarovanja bistveno krajša;
- **obsežnejši nabor kritij za osebne predmete**, ki so ukradeni/izgubljeni skupaj s plačilno kartico. Omenjeno kritje bi prispevalo tudi k spodbujanju potrebe po zavarovanju, saj nas je večji del potrošnikov dandanes obsedenih s svojimi »tehnološkimi igračkami«.

Menim, da bi se imetniki plačilnih kartic z vključitvijo omenjenih kritij za tovrstne zlorabe v ponudbo zavarovalnih produktov počutili varnejše. Glede na široko uporabo plačilnih

kartic v internetnem prostoru ter nov način plačevanja z brezstičnimi karticami ugotavljamo, da so prav to kritja, ki jih zavarovalni prostor v Sloveniji nujno potrebuje. Poleg zaščite finančnih sredstev na plačilni kartici (bančnem računu) pa zavarovalnice svoje produkte obogatijo z vrstami drugih kritij, ki niso neposredno vezana na zlorabo plačilne kartice, pač pa predstavljajo dodatno ugodnost za oškodovanca v primeru izgube/kraje osebnih predmetov skupaj s plačilno kartico. Vsa ta kritja sicer zvenijo privlačno, vendar so za zaščito zlorabe plačilne kartice povsem neuporabna. Menim, da bi moralo zavarovanje biti ločeno glede na to, ali gre neposredno za zlorabo plačilnega instrumenta, druga vrsta zavarovanja pa bi na primer obsegala samo kritje izgube/kraje osebnih predmetov in ne bi vključevala neposredne zlorabe kartice, pač pa samo stroške preklica in izdaje nove kartice. Nekatere zavarovalnice v tujini ponujajo pester nabor kritja za osebne predmete, česar zavarovatelji v Sloveniji v produkte še ne vključujejo v takšnem obsegu. Vrste kritja, ki so prisotne v ponudbi v tujini, v Sloveniji pa še ne, so: kritje škode MP3/MP4-predvajalnika, fotoaparata, telefona, prenosnega računalnika, očal itd. Pri zavarovanju osebnih predmetov je pri zavarovateljih v Sloveniji še veliko prostora za spremembo vrste kritij ter določitev limitov za posamično kritje, odločitev pa je odvisna od zavarovateljev.

SKLEP

V magistrskem delu ugotavljam, da delež globalnega brezgotovinskega poslovanja iz leta v leto narašča in v EU predstavlja že kar 46 % vseh opravljenih transakcij (European Central Bank, 2015b). Potrošniki se niti ne zavedamo vseh mogočih oblik zlorab, ki nas obkrožajo na vsakem koraku uporabe kartice. Pregled oblik zlorab je zato prikazal razsežnosti tovrstne goljufije, saj se zlorabe lahko izvede na mnogo načinov. Kot goljufi se v današnjem obdobju pojavljajo globalne kriminalne združbe z visokim tehnološkim znanjem, zato niti ni presenetljivo, da navkljub prizadevanju izdajateljev po večji varnosti kartičnega poslovanja še vedno prihaja do zlorab. Izdajatelji venomer vnašajo novosti v poslovanje, prav tako poskušajo zagotavljati vedno nove in boljše varnostne ukrepe. Kljub temu kriminalcem uspe zlorabiti marsikatero plačilno kartico. Velik premik pri preprečevanju zlorab je izdajateljem uspel z uvedbo obveznega standarda EMV, s čimer se je delež zlorab, kjer je potrebna fizična prisotnost kartice, nekoliko znižal. Težava je v tem, da so se goljufi prav zaradi težje izvedbe CP-zlorabe preselili v kibernetski prostor (CNP-zlorabe).

Vsako zlorabo plačilne kartice se obravnava individualno, odvisno od poteka dogodkov, kjer se določi morebitna škodna odgovornost imetnika kartice, ki pa po zakonu ne sme presegati 150 EUR. Če se v postopku določi, da škodno odgovornost nosi imetnik kartice, lahko ta poišče zaščito svojega premoženja pri zavarovalnicah, ki ponujajo zavarovanje plačilnih kartic. Zavarovalnice oziroma banke, ki tržijo produkte zavarovalnic, ponujajo različne možnosti tovrstnih zavarovanj. Ob tem je potrebno opozorilo, da je vsaka ponudba zavarovalnice, ki limit za posamičen škoden dogodek za zlorabo kartice postavlja višje od

150 EUR, zavajajoča. Ponudba je mogoče vabljava za imetnika, saj je ta povečini prava neuka stranka in se svojih pravic ne zaveda, zato takšno ponudbo sprejme. Glede na pregled konkurence v tujini je tudi za zavarovalnice v Sloveniji smiselno, da svoje zavarovalne produkte posodobijo, jih naredijo tehnologiji prilagodljive ter za potrošnike privlačnejše, hkrati pa v pogojih jasno opredelijo, da zavarovalnica izplača le tisti del odgovornosti, za katero je odgovoren posameznik.

LITERATURA IN VIRI

1. "Nov" način zlorabe plačilnih kartic. Najdeno 14. februarja 2016 na spletnem naslovu <http://www.monitor.si/novica/nov-nacin-zlorabe-placilnih-kartic/170287/>
2. 3D Secure. Najdeno 13. februarja 2016 na spletnem naslovu https://www.mastercard.com/gateway/implementation_guides/3D-Secure.html
3. Alhothaily, A., Bie, R., Cheng, X., & Alrawais, A. (2015). A novel verification method for payment card systems. *Personal & Ubiquitous Computing*, 19(7), 1145–1156.
4. Anderson, R., & Murdoch, S. J. (2014). EMV: Why Payment Systems Fail? *Communications of the ACM*, 57(6), 24–28.
5. Banka Koper, d.d. (2013). *Pogodba e-trgovina*. Najdeno 21. aprila 2016 na spletnem naslovu http://martinstrel.si/ol.net/bankakoper/MartinStrel_SP_Prodajno_Mesto_Apr2013.pdf
6. Banka Slovenije. (2015). *Bilten banke Slovenije*, 24(12), str. 43.
7. Banka Slovenije. (2016). *Bilten banke Slovenije*, 25(1), str. 43.
8. Bernik, I., & Prisljan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Maribor: Fakulteta za varnostne vede.
9. Bhatla, T. P., Prabhu, V., & Dua, A. (2003, junij). *Understanding Credit Card Frauds*. Najdeno 4. aprila 2016 na spletnem naslovu http://www.popcenter.org/problems/credit_card_fraud/pdfs/bhatla.pdf
10. *Brezstično poslovanje*. Najdeno 20. februarja 2016 na spletnem naslovu <http://www.zbs-giz.si/system/file.asp?FileId=872>
11. Brody, R. G., Brown, D. M., Chettry, A., & White, W. (2014). Proliferation of Credit Card Fraud with Current Technological Advances. *Insights to a Changing World Journal*, 2014(2), 92–107.
12. Calder, A., & Carter, N. (2008). *PCI DSS: A Pocket Guide*. Ely: IT Governance Publishing.
13. Capgemini. (b.l). *Number of Worldwide Non-Cash Transactions for North America, Europe, Mature APAC, Latin America, CEMEA and Emerging Asia in 2009, 2010, 2011, 2012, 2013 and 2014E*. Najdeno 14. marca 2016 na spletnem naslovu <https://www.worldpaymentsreport.com/reports/noncash>
14. Carbo-Velvedere, S., & Rodriguez-Fernandez, F. (2014). ATM withdrawals, debit card transactions at the point of sale and the demand for currency. *SERIEs* 5(4), 399–417.
15. *Card security product holders: claim compensation by 18 March 2016*. Najdeno 16. marca 2016 na spletnem naslovu <https://www.fca.org.uk/news/affinion-scheme-for-card-security-product-holders>
16. Cheney, J. S., Hunt, R. M., Jacob, K. R., Porter R. D., & Summers, B.J. (2012). The efficiency and integrity of payment card systems: Industry views on the risks posed by data breaches. *Economic Perspectives*, 36(4), 130–146.
17. Citibank Czech Republic, a.s. (2016). *Fraudulent usage Insurance 50*. Najdeno 22. februarja 2016 na spletnem naslovu http://www.citibank.com/czech/gcb/personal_banking/english/insurance/insurance_50.htm

18. *Credit Card Fraud Statistic*. Najdeno 27. januarja 2016 na spletnem naslovu <http://www.statisticbrain.com/credit-card-fraud-statistics/>
19. Crossman, P. (2015, 10. november). Why Is the U.S. Taking So Long to Migrate to Chip Cards. *American Banker*. Najdeno 27. januarja 2016 na spletnem naslovu <http://www.americanbanker.com/news/bank-technology/why-is-the-us-taking-so-long-to-migrate-to-chip-cards-1077765-1.html>
20. D'Arcy, J., Hovan, A., & Galleta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98.
21. *Do you need credit card loss insurance or another credit card scam?* Najdeno 15. marca 2016 na spletnem naslovu <http://www.nomoredebts.org/blog/credit/do-you-need-credit-card-loss-insurance-or-another-credit-card-scam.htm>
22. Dulc Strahinič, N. (2014, december). Kam izginjajo plačilne kartice? *Nova Ljubljanska Banka d.d.* Najdeno 14. februarja 2016 na spletnem naslovu <https://www.nlb.si/kam-izginjajo-placilne-kartice>
23. Ergo zavarovalnica, podružnica v Sloveniji. (2015, 1. sept). *Splošni pogoji za zavarovanje imetnikov plačilnih kartic* SP-ERG_ZIK/4. Ljubljana: Ergo zavarovalnica, podružnica v Sloveniji.
24. European Central Bank. (2015a, julij). *Fourth report on card fraud*. Najdeno 17. februarja 2016 na spletnem naslovu https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf
25. European Central Bank. (2015b, 12. oktober). *Payment Statistics for 2014*. Najdeno 17. februarja 2016 na spletnem naslovu <https://www.ecb.europa.eu/press/pdf/pis/pis2014.en.pdf?d9feb0268bb38b960b806ea69b6bf467>
26. Evans, D. S., & Schmalensee, R. (2009). Innovation and Evolution of the Payment Industry. V R. E. Litan & M. Neil Bailey (ur), *Moving money : the future of consumer* (str. 36–76). Washington, D.C.: The Brookings Institutions.
27. Evropski ekonomsko-socialni odbor. (2012, 19. september). *Mnenje Evropskega ekonomsko-socialnega odbora o zeleni knjigi Na poti k integriranem evropskem trgu za kartična, spletna in mobilna plačila COM(2011) 941 final*. Najdeno 10. marca 2016 na spletnem naslovu https://www.google.si/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj9vrFs8HMAhUpBMAKHeomDn8QFggaMAA&url=https%3A%2F%2Fwebapi.eesc.europa.eu%2Fdocumentsanonymous%2Fces1241-2012_00_00_tra_ac_sl.doc&usg=AFQjCNF6hGMHCNaUQ3ckFuUpRx-E3KVzQ&sig2=GhDm-_yQkX1Y_z2bAtIk_w&bvm=bv.121099550,d.ZGg
28. Financial Fraud Action UK. (2015). *Fraud The Facts 2015. The definitive overview of payment industry fraud and measures to prevent it*. Najdeno 13. marca 2016 na spletnem naslovu <http://www.financialfraudaction.org.uk/publications/ftf/#1>
29. Flis, S. (1999). *Zbrani spisi o zavarovanju* (IV. knjiga). Ljubljana: Slovensko zavarovalno združenje, GIZ.

30. *Fraud Insurance for Payment Cards*. Najdeno 10. marca 2016 na spletnem naslovu <https://www.sberbankcz.cz/en/Individuals/pojisteni-ke-kartam/pojisteni-karty-a-osobnich-veci>
31. Generali zavarovalnica, d.d. Ljubljana. (2010). *Splošni pogoji za zavarovanje imetnikov kartice Diners Club*. Ljubljana: Generali zavarovalnica, d.d. Ljubljana.
32. Glas, A. (2012). *Varnost kartičnega poslovanja – PCI DSS (payment card industry data security standard)*. Prispevek predstavljen na Dnevih slovenske informatike 2012. Najdeno 5. februarja 2016 na spletnem naslovu <http://fmc.si/Documents/Fmc/VARNOST%20KARTI%C4%8CNEGA%20POSLOVANJA%20%E2%80%93%20PCI%20DSS.pdf>
33. Greenberg, A. (2012, 30. januar). Hacker's Demo Shows How Easily Credit Cards Can Be Read Through Clothes And Wallets. *Forbes Magazine*. Najdeno 27. januarja 2016 na spletnem naslovu <http://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/#3bac54177fc2>
34. Holmes, T. E. (2015, 16. september). Credit card fraud and ID theft statistics. *CreditCards.com*. Najdeno 31. januarja 2016 na spletnem naslovu <http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>
35. *Insurance against misuse of a card*. Najdeno 10. marca 2016 na spletnem naslovu <http://www.kb-pojistovna.cz/en/insurance/insurance-in-payment-cards/insurance-against-misuse-of-vega-card/description.shtml>
36. J. Mann, R. (2006). *Charging Ahead: The Growth and Regulation of Payment Card Markets Around the World*. Cambridge: Cambridge University Press.
37. *Kaj je skimming?* Najdeno 20. februarja 2016 na spletnem naslovu <http://www.bankart.si/si/pomoc/faq/>
38. *Kartice*. Najdeno 4. aprila 2016 na spletnem naslovu http://www.sepa.si/SloPrenova/SepaProdukti_Storitve/Kartice/SepaProdukti%20in%20storitve_Kartice.htm
39. Kitten, T. (2015, 18. november). Why Fraudsters Have Shifted to 'Shimming' Attacks. *Bank Info Security*. Najdeno 22. februarja 2016 na spletnem naslovu <http://www.bankinfosecurity.com/blogs/banks-prevent-shimming-losses-p-1980/op-1>
40. Kjos, A. (2007, 28. november). The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges. *Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 07-12*. Najdeno 28. januarja 2016 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1031519
41. Kobs, K. (2015). EMV is Here – Is Your Business Ready? *Franchising World*, 47(8), 47–48.
42. Koma (2001). *Priročnik o opravljanju plačilnega prometa med banko in komitentom z navodili*. Kamnik: Izdajanje poslovnih publikacij, podjetniško in poslovno svetovanje.
43. Kovač, M. (2011). *Plačilni sistem in plačilna disciplina*. Maribor: De Vesta.

44. Krisper, B., & Meško, A. (2015, 4. junij). Predplačniške kartice – najprej plačam, potem kupujem. *Zveza potrošnikov Slovenije*. Najdeno 15. januarja 2016 na spletnem naslovu <https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/73-72-predplacniske-kartice-najprej-placam-potem-kupujem-5-2015>
45. Lamb, E. C. (2001). Debit Cards. *Community Banker*, 10(2), 18.
46. Lamberger, I. (2009). *Gospodarski kriminal*. Ljubljana: Fakulteta za varnostne vede.
47. Lamberger, I. (2011). *Model zaščite elektronskih plačilnih sistemov pred zlorabami* (doktorska disertacija). Ljubljana: Ekonomska fakulteta.
48. Lamberger, I., Dobovšek, B., & Slak, B. (2012). Zlorabe plačilnih kartic – pogledi izdajateljev kartic. *Revija za kriminalistiko in kriminologijo*, 63(2), 123–135.
49. *Lost Wallet Protector from American Express*. Najdeno 10. marca 2016 na spletnem naslovu <https://lwpenroll.americanexpress.com/offer.cfm?siteID=88888&sid=AX0212558337>
50. Lubej, R. (2014, 15. april). Do varnosti podatkov s tokenizacijo. *STA d.o.o.* Najdeno 6. aprila 2016 na spletnem naslovu <http://www.o-sta.com/msg.php?id=13185>
51. *Maestro kartica*. Najdeno 12. januarja 2016 na spletnem naslovu <http://www.mastercard.com/si/consumer/maestro.html>
52. *Maintaining payment security*. Najdeno 20. februarja 2016 na spletnem naslovu https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
53. Marshall, E. A., & Lattin, M. (2015). Understanding the Payment Card Fraud Liability Shif. *Commercial & Business Litigation*, 17(1), 15–18.
54. Maurer, D. (2009). An examination of the economics of payment card system. *Swiss National Bank*. Najdeno 24. decembra 2015 na spletnem naslovu <http://www.snb.ch/en/mmr/reference/Zahlungskarten/source/Zahlungskarten.en.pdf>
55. Medveš, A. (2014). Pomen projektnega vodenja v zavarovalništvu. *Zavarovalniški horizonti*, 10(1), 61–71.
56. Munich Re Group. (2001). *Bancassurance in practice*. München: Münchener Rückversicherungs-Gesellschaft.
57. Odar, M. (2000). Kreditne (zaupanjske) kartice. *IKS revija za računovodstvo in finance*, 27(9), 93-107.
58. OECD. (2002). Report on Consumer Protections for Payment Cardholders. *OECD Digital Economy Papers No.64*. Najdeno 17. novembra 2015 na spletnem naslovu http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/report-on-consumer-protections-for-payment-cardholders_233364634144#page1
59. Pavia, J. M., Veres-Ferrer, E. J., & Foix-Escura, G. (2012). Credit card incidents and control systems. *International Journal of Information Management*, 32(6), 501–503.
60. *Payment cards*. Najdeno 26. januarja 2016 na spletnem naslovu <http://www.interpol.int/Crime-areas/Financial-crime/Payment-cards>
61. Payments cards and mobile. (2015). *Card Fraud Report*. Najdeno 10. marca 2016 na spletnem naslovu http://www.paymentscardsandmobile.com/wp-content/uploads/2015/03/PCM_Alarc_Fraud-Report_2015.pdf

62. *PCI Compliance Guide.org*. Najdeno 11. februarja 2016 na spletnem naslovu <https://www.pcicomplianceguide.org/pci-faqs-2/#1>
63. PCI Security Standards Council. (2013). *Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures*. Version 3.1
64. PCI Security Standards Council. (2014). *PCI DSS Quick Reference Guide*. Najdeno 13. februarja 2016 na spletnem naslovu <https://www.pcisecuritystandards.org/documents/PCISSC%20QRG%20August%202014%20-print.pdf>
65. *Plačilne kartice*. Najdeno 23. decembra 2015 na spletnem naslovu http://www.mojdenar.com/BANKE/plac_kart_splosno.asp
66. *Plačilni in poravnalni sistemi*. Najdeno 11. januarja 2016 na spletnem naslovu <http://www.bsi.si/placilni-sistemi.asp?MapaId=1427>
67. *Plačilni instrumenti*. Najdeno 11. januarja 2016 na spletnem naslovu <https://www.bsi.si/placilni-sistemi.asp?MapaId=1431>
68. Potočnik, V. (2004). *Trženje storitev s primeri iz prakse* (2. izdaja). Ljubljana: GV založba.
69. *Pozor: najbolj množičen in sofisticiran phishing napad v Sloveniji*. Najdeno 30. januarja 2016 na spletnem naslovu <https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/7222-pozor-najbolj-mnozicen-in-sofisticiran-pishing-napad-v-sloveniji>
70. *Premoženjska zavarovanja*. Najdeno 2. marca 2016 na spletnem naslovu <https://www.dbs.si/produkt/premozenjska-zavarovanja-129>
71. Pust, J. (2009). Razvoj zavarovalnih produktov. *Zavarovalniški horizonti*, 5(1), 21–36.
72. Quah, J. T. S., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert Systems with Applications*, 35, 1721–1732.
73. Rizmal, I. (2008). *Spletna trgovina v okolju ASP.NET*. Kranj: Fakulteta za organizacijske vede.
74. Robertson, D. A. (2014). Safe to Swipe?: Why Congress Should Amend the EFT A to Increase Debit Card User Protection. *Texas Law Review*, 93(2), 505–519.
75. RSA. (2014). *Card-Not-Present Fraud in a Post-EMV*. Najdeno 13. februarja 2016 na spletnem naslovu <https://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf>
76. Ruark, C. A. (2015). Upgrade or else (cover story). *Las Vegas Business Press* 32(15), 18–19.
77. Slabe Cepec, M., & Lekše, M. (2009). *Računovodstvo in finančno poslovanje*. Ljubljana: Zavod IRC.
78. Slawsky, J., & Zafar, S. (2005). *Developing and Managing a Successful Payment Card Business*. Aldershot: Gower Publishing Limited.
79. Souvignet, T., Hatin, J., Maqua, F., Tesniere, D., Leger, P., & Hormiere, R. (2014). Payment card forensic analysis: From concepts to desktop and mobile analysis tools. *Digital Investigation*, 11(3), 143–153.
80. Sullivan, R. J. (2008). Can smart cards reduce payments fraud and identity theft? *Economic Review*, 93(3), 35–62.

81. Sullivan, R. J. (2013). The U.S. Adoption of Computer-Chip Payment Cards: Implication for Payment Fraud. *Economic Review*, 2013(1), 59–87.
82. Šavnik, J. (2008). *Varnost negotovinskega poslovanja*. Ljubljana: Zveza potrošnikov Slovenije.
83. Šteblaj, A. (1999). Uporaba sodobnih plačilnih instrumentov v Sloveniji v prvem polletju 1999. *Prikazi in analize*, 7(3), 41–59.
84. *Temeljna pravila varne uporabe kartic*. Najdeno 13. marca 2016 na spletnem naslovu <http://www.zbs-giz.si/news.asp?StructureId=1216&ContentId=7940>
85. The Nilson Report. (2015). *Purchase Transactions On Global Cards 2013*. Najdeno 13. marca 2016 na spletnem naslovu https://www.nilsonreport.com/publication_special_chart.php
86. *The What, Who and Why of Contactless Payments*. Najdeno 5. februarja 2016 na spletnem naslovu <http://www.smartcardalliance.org/publications-contactless-payments-what-who-why/>
87. *Types of credit card fraud*. Najdeno 27. januarja 2016 na spletnem naslovu <http://www.monetos.co.uk/financing/credit-cards/fraud-protection/>
88. *Udobni paketni računi*. Najdeno 2. marca 2016 na spletnem naslovu <http://www.sparkasse.si/udobni-paketni-racun>
89. *Understanding Chargeback*. Najdeno 16. marca 2016 na spletnem naslovu <https://www.dalpay.com/en/support/chargebacks.html>
90. UniCredit Bank Czech Republic and Slovakia. (2015). *Insurance against card misuse*. Najdeno 11. marca 2016 na spletnem naslovu https://www.unicreditbank.cz/files/download/pojisteni/Prehled_pojistnych_limitu_SAFE_Generali_EN.pdf
91. Uniqa Versicherungen AG (2012). *Splošni pogoji zavarovanja uporabnikov kreditno plačilnih kartic*. Klagenfurt am Wörthersee: Uniqa Versicherungen AG.
92. Vermeulen, P. (2004). Managing Product Innovation in Financial Services Firms. *European Management Journal*, 22(1), 43–50.
93. Vičič, M. (2005). Bančno zavarovalništvo – nove prodajne poti. *Zavarovalniški horizonti*, 1(2), 57–72.
94. Voh Boštič, A. (2015, 11. avgust). Kiberkriminal v Sloveniji (2): zakaj je boljša varnost vzrok za več zlorab bančnih kartic. *Pod črto*. Najdeno 30. oktobra 2015 na spletnem naslovu <https://podcrto.si/kiberkriminal-v-sloveniji-2-zakaj-je-boljsa-varnost-vzrok-za-vec-zlorab-bancnih-kartic-2/>
95. Woolsey, B., & Gerson, E.S. (2009, 11. maj). The history of credit cards. *CreditCards.com*. Najdeno 23. decembra 2015 na spletnem naslovu <http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php>
96. Zakon o plačilnih storitvah in sistemih. *Uradni list RS* št. 58/09, 34/10, 9/11, 32/12 in 81/15.
97. Zavarovalnica Maribor, d.d. (2010). *Splošni pogoji za zavarovanje nevarnosti izgubljenih ali ukradenih plačilnih ali kreditnih kartic*. Maribor: Zavarovalnica Maribor, d.d.

98. Zavarovalnica Tilia, d.d. (2014). *Pogoji za zavarovanje zavarovalnega programa Zavarovanje kartic plus*. Novo mesto: Zavarovalnica Tilia, d.d.
99. Zavarovalnica Triglav, d.d. (2012). *Posebni pogoji za zavarovanje plačilnih kartic. PG-kpk-12-10*. Ljubljana: Zavarovalnica Triglav, d.d.
100. *Zavarovanje kartic in osebnih predmetov*. Najdeno 2. marca 2016 na spletnem naslovu <https://www.nkbm.si/zavarovanje-kartic-osebni-predmetov>
101. *Zavarovanje kartic plus*. Najdeno 2. marca 2016 na spletnem naslovu <https://www.skb.si/osebne-finance/kartice/zavarovanje-kartic-plus>
102. *Zavarovanje kartic*. Najdeno 1. marca 2016 na spletnem naslovu <http://www.abanka.si/zavarovanje-kartic/>
103. *Zavarovanje uporabnikov kartic*. Najdeno 1. marca 2016 na spletnem naslovu <http://www.hypo-alpe-adria.si/content/zavarovanje-uporabnikov-kartic>
104. *Zavarovanje za primer izgube ali kraje kartice*. Najdeno 2. marca 2016 na spletnem naslovu <https://www.nlb.si/zavarovanje-izguba-kraja-kartice>
105. Završnik, A. (2015). *Kibernetika kriminaliteta*. Ljubljana: GV Založba.
106. Združenje bank Slovenije. (2011, 18. marec). *Slovarček strokovnih izrazov za področje kartičnega poslovanja*. Najdeno 13. marca 2016 na spletnem naslovu http://www.sepa.si/SloPrenova/Gradiva_Publikacije/Sepa_Zbs/SlovarSepa_KarticeSloAng.pdf
107. Zelenik, A., & Mezgec, Z. (2009). Zaščita negotovinskih oblik plačevanja. *Uporabna informatika*, 17(4), 265–278.
108. *Zgodovina pametnih kartic*. Najdeno 23. decembra 2015 na spletnem naslovu <http://www.activa.si/pametnaKartica/zgodovina.asp>
109. Zupančič, M. (1999). Zlorabe plačilnih kartic pri elektronskem poslovanju. *Revija za kriminalistiko in kriminologijo*, 50(3), 215–224.
110. Žagar, G. (2011). Kako varno je nakupovanje na spletu. *Bančni vestnik*, 60(7/8), 20–25.
111. Žnidarič, B. (2004): *Zavarovalništvo in varnost*. Ljubljana: Fakulteta za družbene vede in Slovensko zavarovalno združenje.