TARTU ÜLIKOOL

Majandusteaduskond

Britta Kiviking

MAKSEPETTUSED JA NENDE TÕKESTAMINE EESTIS

Bakalaureusetöö

Juhendaja: dotsent Nadežda Ivanova

Tartu 2016

Soovitan suunata kaitsmisele ……..

(juhendaja nimi)

Kaitsmisele lubatud “ “..... 2016. a.

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

……..

(töö autori nimi)

SISUKORD

SISSEJUHATUS

Iga päev teostatakse sularahaga ning sularahata makseid, kuid maksevahendite kasutamisel ning tehingute teostamisel ei mõelda võimalikele riskidele. Üks riskidest, mis on seotud maksesüsteemide ja maksevahenditega, on pettuse risk. Pettused on eksisteerinud sama kaua kui pangad ning alati leidub kurjategijaid, kes üritavad maksesüsteeme murda. Pankadel on vaja kaitsta nii ennast kui ka oma kliente, seega rakendatakse erinevaid maksepettuste tõkestamismeetmeid. Käesolev bakalaureusetöö teema on väga aktuaalne, kuna maksepettuste arv jätkuvalt kasvab. Bakalaureusetöös keskendutakse pankade poolt kasutusele võetud maksepettuste tõkestamismeetmetele, mis aitavad kaitsta pankasid ning panga kliente võimalike ohtude eest.

Bakalaureusetöös on vaatluse all kolm peamist sularahata maksevahendit, mida ohustavad kurjategijad, nimelt, tšekid, pangaülekanded ning maksekaardid. Töös käsitletakse kõiki kolme maksevahendit ning nendega seotud pettuseid. Bakalaureusetöös keskendutakse peamiselt maksekaardipettustel, kuna Euroopa Keskpanga aruannete kohaselt on maksekaardid kõige laialdasemalt kasutatav sularahata maksevahend Euroopa Liidu riikides.

Bakalaureusetöö eesmärk on välja selgitada maksepettuste eripära Eestis ning selle seos tõkestamismeetmetega. Oluline on välja selgitada, kas maksepettused kujutavad suurt ohtu Eestis ning milliseid tõkestamismeetmeid rakendatakse pettuste vältimiseks.

Bakalaureusetöös uuritud teema võib pakkuda huvi kõikidele, kes kasutavad sularahata maksevahendeid. Bakalaureusetöö aitab mõista maksepettuste probleemi tõsisust ja võimalike ohte ja skeeme, mille ohvriks on võimalik langeda. Tegemist on väga keerulise teemaga, kuna suur osa informatsiooni on konfidentsiaalne. Seega autor esitas endale väljakutse kirjutada teemal, millest varasemalt pole üliõpilastöid kirjutatud. Kuna valitud teema on väga lai ning pidevalt arenev, on bakalaureusetööd võimalik arendada ka magistritööks.

Eesmärgi saavutamiseks on autor püstitanud järgmised uurimisülesanded:

- defineerida maksepettuste sisu,
- esitada ja selgitada maksevahenditega seotud pettuseid,
- erialakirjanduse alusel esitada maksepettuste võimalikud tõkestamismeetmed,
- välja selgitada maksepettuste levik ning eripära Eestis,
- autori küsitluse abil selgitada välja maksepettuste tõkestamismeetmed Eestis,
- võrrelda küsitluse tulemusi teoreetilises osas tooduga ning esitada soovitused maksepettuste vähendamiseks.

Teoreetilise osa koostamiseks kasutab autor EBSCO, ESTER-i ja Google Scholari andmebaase ja otsingumootoreid, et leida teemakohaseid teadusartikleid maksepettuste kohta. Peamised kirjandusallikad on võõrkeelsed, nimelt inglise keelsed. Empiirilise osa koostamiseks kasutab autor maksepettuste kohta avaldatud statistikat ning koostab varasemate uuringute põhjal küsimustiku, et teada saada maksepettuste tõkestamismeetmete kohta Eestis.

Varasemalt on Tartu Ülikooli Majandusteaduskonnas kirjutatud bakalaureusetöö pangakaardipettuste teemal, milles keskenduti peamiselt kaardiomanike poolt kasutatavatele meetmetele, et vältida kaardipettuse ohvriks langemist. Käesolevas bakalaureusetöös aga keskendutakse pankade poolt kasutusele võetud maksepettuste tõkestamismeetmetele. Samuti on vaatluse all lisaks maksekaartidele ka tšekid ja pangaülekanded.

Bakalaureusetöö koosneb kahest peatükist. Esimeses ehk teoreetilises peatükis selgitatakse maksepettuste sisu ning konkreetsete maksevahenditega seotud pettuseid. Samuti esitatakse maksepettuste võimalikud tõkestamismeetmed. Töö teises peatükis uuritakse maksepettuste levikut Eestis ning selgitatakse välja, millised maksepettuste tõkestamismeetmed on kasutusel Eestis. Autor näeb väga head võimalust uurida aktuaalset ning uudset teemat, mida varasemalt pole uuritud.

Tööd iseloomustavad märksõnad: maksepettus; maksekaart; tšekk; pangaülekanne; tõkestamismeetmed

1. MAKSEPETTUSED JA NENDE TÕKESTAMISE TEOREETILINE KÄSITLUS

1.1. Maksepettus ning selle liigid

Mõiste „maksepettus“ tähendus tundub lihtne ning arusaadav, kuid tegelikkuses on see keerulisem kui pealtnäha tundub. Selles alapeatükis esitatakse erinevate autorite definitsioonid vaatlusaluse mõiste kohta. Samuti esitatakse definitsioonide võrdlus, et paremini mõista maksepettuse sisu ning leida mõiste erinevaid käsitlusviise. Lisaks definitsioonidele, tuuakse välja maksevahendid, mida kõige enam ründavad kurjategijad ning selgitatakse maksevahenditega seotud pettuseid.

Igas majanduses toimub iga päev suur hulk maksetehinguid. Kõikidel maksetehingutel, vaatamata sellele, kas tegemist on kauba või teenuse soetamisega, on kaks osa (eeldusel, et ei hõlma vahetuskaupa) (The Payment System 2010: 25):

- kaupade või teenuste üleandmine;
- rahaliste vahendite ülekanne- st maksmisel kasutatakse sularaha või pangakontol olevat raha.

Seega makse on rahaliste vahendite ülekanne, kus üheks tehingu osapooleks on maksja, kes nõustub rahaliste vahendite ülekandega makse saajale. Teine osapool on aga makse saaja, kes on lõplik raha saaja. (The Payment System 2010: 25)

Internetis leiduv Oxfordi sõnaraamat defineerib pettust kui kriminaalset tegevust, eesmärgiga saada finantsilist või isiklikku kasu (Fraud 2016). Vaatamata märkimisväärsetele edusammudele pettust avastavas tehnoloogias, kujutavad pettusest tulenevad kahjud jätkuvalt tõsist probleemi (Chiezey, Onu 2013: 13).

Bakalaureusetöö läbivaks mõisteks on maksepettus, seega on oluline mõistet defineerida. Selleks on autor koostanud tabeli 1, kus on viie autori poolt esitatud definitsioonid maksepettuse kohta. Bakalaureusetöö autor on valinud definitsioonid erinevatest

allikatest, eesmärgiga leida erinevaid lähenemisviise ja vaatenurki mõistele. Esimesed kolm definitsiooni pärinevad teadusartiklitest. Neljas definitsioon pärineb Europoli koduleheküljelt. Autor teab, et Europol on Euroopa Liidu õiguskaitseasutus ning autor peab allikat usaldusväärseks. Viies definitsioon on USLegal koduleheküljelt. Valitud on USLegali poolt esitatud definitsioon, eesmärgiga võrrelda erinevaid definitsioone.

Tabel 1. Maksepettuse definitsioonid

AUTOR	DEFINITSIOON
Sullivan (2010: 103)	Maksepettus toimub siis, kui saadakse rahalist või materiaalset kasu, kasutades tehingute teostamiseks maksevahendit (või maksevahendilt saadud informatsiooni), millele ei ole juurdepääsu andnud õiguslik maksevahendi omanik.
Gates, Jacob (2009: 7)	Maksepettust võib üldiselt defineerida kui tegevust, kus kasu saamise nimel kasutatakse ebaseaduslikult mistahes maksetehingute informatsiooni.
Dhameja, Jacob, Porter (2013: 108-109)	Maksepettust, mis võib avalduda erinevatel viisidel, saab üldjoontes defineerida kui mistahes tegevust, milles kasu saamise nimel kasutatakse ebaseaduslikult konfidentsiaalset isiklikku (või finantsilist) informatsiooni. Sealhulgas kurjategijad algatavad tehinguid ilma omaniku nõusolekuta või autorisatsioonita.
Europol (Payment Fraud 2016)	Maksepettused ja internetipettused on väga tulus kriminaalne tegevus, mida iseloomustab kaks metoodikat, sõltuvalt sellest, kas maksekaart on pettuse ajal füüsiliselt olemas või mitte.
USLegal (Payment Fraud Law & Legal Definition 2016)	Maksepettus viitab pettusele, mis leiab aset siis, kui pettuslike tehinguid teostatakse maksekaardiga. Esineb konto ülevõtmise tagajärjel või võltsitud kaardi kasutamise tulemusena.

Allikas: Autori koostatud Sullivan (2010: 103); Gates, Jacob (2009:7); Dhameja, Jacob, Porter (2013:108-109); Europol (Payment Fraud 2016); USLegal (Payment Fraud Law & Legal Definition 2016) põhjal.

Tabeli 1 põhjal võib mõista, et definitsioonid on üksteist täiendavad, kuid ei erine suuresti teineteisest. USLegal-i poolt esitatud definitsioon (Payment Fraud Law & Legal Definition 2016) on ainuke, mis selgitab, et maksepettus esineb konto ülevõmise tagajärjel või võltsitud kaardi kasutamise tulemusena. Europoli (Payment Fraud 2016) poolt esitatud definitsioon on autori arvates üldine, kuid selgitab, et maksepettuseid iseloomustab kaks metoodikat. Teadusartiklitest esitatud definitsioonid (Sullivan 2010: 103; Gates, Jacob 2009: 7; Dhameja *et al.* 2013: 108-109) on sarnased ning kõikides definitsioonides väidetakse, et maksepettuse eesmärgiks on kasu saamine ning

ebaseaduslikult kasutatakse maksevahendeid või maksevahendite informatsiooni. Nagu tabelist 1 on näha, USLegali poolt esitatud definitsioon (Payment Fraud Law & Legal Definition 2016) ei erine suuresti teadusartiklites esitatud definitsioonidest.

Bakalaureusetöös kasutatakse Sullivani (2010: 103) poolt esitatud definitsiooni, nimelt maksepettus toimub siis, kui saadakse rahalist või materiaalset kasu, kasutades tehingute teostamiseks maksevahendit (või maksevahendilt saadud informatsiooni), millele ei ole juurdepääsu andnud õiguslik maksevahendi omanik. Autori arvates on see definitsioon kõige sobilikum, kuna definitsioon on konkreetne ning võtab kokku tabelis 1 esitatud definitsioonid.

Olles tutvunud ning võrrelnud maksepettuse erinevaid definitsioone, selgitatakse järgnevalt kahte viisi, kuidas maksepettuseid on võimalik jagada. Nimelt, maksepettuseid on võimalik jaotada (Gates, Jacob 2009: 7):

- esimese osapoole pettus (*first-party fraud*);
- kolmanda osapoole pettus (*third-party fraud*).

Esimese osapoole pettus ilmneb, kui pettus on teadlikult toime pandud tarbija poolt (Gates, Jacob 2009:7). Näiteks, kaardipettuse korral kaardiomanik tahtlikult ei tagasta pangale laenu (Card-Not-Present Fraud... 2014: 5). Kolmanda osapoole pettuse korral satub tarbija petturite ohvriks (Gates, Jacob 2009:7). Ehk maksepettus pannakse toime isiku poolt, kes pole maksevahendi legitiimne omanik (Sullivan 2014: 7). Bakalaureusetöös on vaatluse all kolmanda osapoole pettused.

Järgnevalt esitatakse maksevahendi selgitus. Samuti esitatakse maksevahendid, mis kalduvad olema kõige suuremas ohus.

On mitmeid erinevaid maksevahendeid, millega on võimalik esitada makse (The Payment System 2010: 25). See võimaldab raha kanda üle maksjalt makse saajale. Kõige levinumad maksevahendid on sularahaga ja sularahata maksed. (The Payment System 2010: 28)

Sularahamaksed (st maksetes kasutatakse rahatähti ja münte) on tavaliselt madala maksumusega näost-näkku tehingud üksikisikute või üksikisiku ja kaupmehe vahel. Sularahata maksed on aga seotud rahaülekannetega kontode vahel. Sularahata maksmise

korral annab maksja pangale ametliku loa raha ülekandmiseks või makse saaja annab pangale juhised raha saamiseks maksjalt. Maksja ja makse saaja pangakontod võivad olla samas või erinevas pangas. (The Payment System 2010: 28)

Engler (2015: 28) väitis, et kõige suuremas ohus kalduvad olema järgmised maksevahendid:

- tšekid;
- maksekaardid;
- pangaülekanded.

Bakalaureusetöös käsitletakse kõiki kolme levinumat maksevahendit ning nendega seotud pettuseid, kuid peamine rõhk on maksekaartidel ja maksekaardipettustel. Autori arvates on maksekaardid kõige rohkem kasutatav maksevahend Euroopa Liidus. Väite kinnitamiseks uuris autor Euroopa Keskpanga poolt avaldatud aruandeid ning selgus, et juba 2012. aastal oli Euroopa Liidus kõige rohkem kasutatav sularahata maksevahend maksekaart (Card payments in Europe... 2014: 25). Järgnevalt on vaatluse all maksekaardipettused.

Maksekaart on seade, mida saab selle omanik kasutada kaupade ja teenuste eest tasumiseks või raha väljavõtmiseks (The Payment System 2010: 343). Maksekaardipettus on aga üldine termin, millega kirjeldatakse erinevaid õigusrikkumisi, mis sisaldavad vargust ja petturlikku maksekaardi andmete kasutamist (Payment cards 2016). Matheswaran, Siva Sankari ning Rajesh definitsioonist võib mõista, et krediitkaardipettus ning maksekaardipettus langevad kokku. Nimelt, krediitkaardipettus on varguse ja pettuse toimepanemise laiaulatuslik termin, mis on seotud maksekaartide, nagu krediitkaardi või deebetkaardi, kasutamisega. Krediitkaardipettuse eesmärgiks võib olla kaupade saamine ilma maksmata või volitamata saada pangakontolt vahendeid. (Matheswaran *et al.* 2015: 11)

Europoli kohaselt on kaks pettuse meetodit, sõltuvalt sellest, kas maksekaart on pettusliku tehingu ajal füüsiliselt olemas või mitte. Pettus, mille korral kaart pole füüsiliselt olemas (edaspidi e-kaubanduspettus) hõlmab andmete volitamata kasutamist (krediitkaardi või deebetkaardi numbri, turvakoodi, aegumiskuupäeva kasutamist) toodete ja teenuste soetamiseks mitte näost-näkku keskkonnas, näiteks e-kaubanduse veebilehekülgelt.

(Payment Fraud 2016) Selliste tehingute korral ei ole võimalik füüsiliselt kontrollida maksekaarti ning võimaldab kaardikasutajal varjata oma tõelist identiteeti (Patidar, Sharma 2011: 33).

Pettus, kus kaart on füüsiliselt olemas (edaspidi pettus müügikohas) hõlmab kaardi magnetriba dubleerimist läbi seadme, mis on peidetud sularahaautomaati või kaardimakseterminali (Payment Fraud 2016). Seega kasutatakse krediitkaarti või deebetkaarti, et teha volitamata tehinguid näost-näkku, näiteks toidupoe kassas (Card present fraud 2016). Näost-näkku makse korral maksja ja makse saaja on samas füüsilises asukohas (The Payment System 2010: 352). Enamasti kaardimakseterminalide ja pangaautomaatide pettused pannakse toime kasutades võltsitud kaarte või varastatud/kaotatud kaarte (Report on card fraud 2012: 4).

Varastatud/kaotatud kaardi pettus hõlmab kaardi ebaõiguslikku kasutamist, mis on varastatud kaardiomanikult või kaardiomaniku poolt kaotatud (Payment cards 2016). Võltsitud kaartide korral aga kasutatakse plastikust kaarte, mis on spetsiaalselt valmistatud või olemasolevaid kaarte on muudetud (Payment cards 2016). Selle pettuse korral on andmed kaardi magnetribalt kopeeritud pangaautomaadis või kaardimakseterminalis läbi *skimmingu* seadme ning kaardi andmeid kasutatakse, et luua võltsitud kaarte. Kriminaalid kasutavad võltsitud kaarte, et osta kaupu edasimüügiks või kui kurjategijatele on teada ka PIN kood, kasutatakse võltsitud kaarte raha välja võtmiseks pangaautomaatidest. (Australian payments fraud 2015:14)

Võltsitud kaardid koos varastatud/kaotatud kaartidega kujutavad kõige suuremat ohtu kaardipettustes. Petturid pidevalt leiavad uusi ja uuenduslikke viise, kuidas luua võltsitud kaarte. Üheks võimaluseks on *skimming*. See on protsess, kus krediitkaardi magnetribal olevad andmed on elektrooniliselt kopeeritud võltskaardile. (Patidar, Sharma 2011: 33)

Olles tutvunud maksekaardipettustega, selgitatakse järgnevalt tšekipettuseid. Tšekk on väljaandja/kontoomaniku poolt kirjutatud korraldus pangale kindla rahasumma maksmiseks nimetatud saajale (Cheques&Cheque Clearing... 2012: 4).

On mitmeid liike tšekipettuseid, mis võivad tabada pankasid ja nende kliente (Turner, Wunnicke 2004: 45). Kolm peamist tšekipettuse liiki on (Fraud the facts 2015: 22):

- võltsitud tšekid,
- muudetud tšekid,
- võltsitud allkirjad.

Samuti Woodfield on väitnud (2013: 18), et tšekipettuste peamiste meetodite hulka kuuluvad võltsitud tšekid, muudetud tšekid ning võltsitud allkirjad. Järgnevalt esitatakse tabel 2, kus on esitatud kolm peamist tšekipettuse liiki ning avatud on nende sisu.

Tabel 2. Tšekipettuste liigid ning kirjeldused

Liik	Kirjeldus
Võltsitud tšekk	Võltsinguga on kavatsetud jäljendada tõelist tšekki tšekiraamatust, mis kuulub pettuse ohvrile. Tänu edusammudele näiteks värvilises kopeerimises, on see kõige kiiremini kasvav tšekipettuse tüüp.
Muudetud tšekk	Pettur muudab tšekki enne selle väljamaksmist, näiteks muutes saaja nime või tšekil olevat summat. Pettus toimub pärast seda, kui kehtivad tšekid on loodud. Pettur kasutab kemikaale või teisi vahendeid, et eemaldada tšekkidelt informatsioon.
Võltsitud allkirjad	Tšekk varastatakse süütult kliendilt ning kasutatakse petturi poolt võltsitud allkirjaga. Tšeki esiküljel võib olla võltsitud või volitamata allkiri või võltsitud/volitamata märge tšeki tagumisel poolel.

Allikas: Autori koostatud Fraud the facts 2015 (2015: 22); Turner, Wunnicke (2004: 45); What you need to know... (2016: 4) põhjal.

Tehnoloogia on teinud kurjategijatele järjest lihtsamaks võltstšekkide loomise, samuti väljamõeldud isikut tõendavate dokumentide loomise, mida saab kasutada tšekipettuse toimepanemiseks (Check Fraud Prevention 2016). Turner ja Wunnicke (2004: 45) on samuti väitnud, et tšekipettuseid on soodustanud odava tarkvara ja riistvara levik, et luua näiteks võltstšekke. Samuti laserprinterid, skännerid ja koopiamasinad tšekkide dubleerimiseks, et tšekid näeksid välja nagu originaalsed tšekid (Turner, Wunnicke 2004: 45).

Olles tutvunud tšekipettustega, selgitatakse järgnevalt viimast kõige levinumat maksevahendit, mida ohutstavad kurjategijad. Selleks on pangaülekanded. Petturlikud

ülekanded võivad avaldada laastavat kahju klientidele ning võivad põhjustada maine kahjustust ja olulist rahalist kahju finantsinstitutsioonidele (Wire fraud prevention 2014: 1).

Ülekandepettuse korral ohvrilt varastatakse isiklikud andmed ning kasutatakse, et algatada volitamata ülekanne (Dhameja *et al.* 2013: 112). Petturlik tehing võib toimuda minutite jooksul, kuid mõju võib kesta mitu kuud, mõnikord ka aastaid, tänu pikkadele ja kulukatele kohtuprotsessidele (Fighting wire fraud... 2013: 2).

Käesoleva bakalaureusetöö kontekstis viitavad ülekandepettused pettuslikule tegevusele, eesmärgiga pääseda ligi ohvri pangakontole ning sealt kanda üle rahalisi vahendeid. Mõningatel juhtudel võib kurjategija petta ohvrit lausa endale ülekannet tegema. (Fraud the facts 2015: 23)

Kuna pangakonto omanikud mitte ainult ei kasuta lihtsaid paroole, vaid kasutatakse samu paroole mitmetes kohtades, on kurjategijatel väga lihtne ohvri pangakontole ligi pääseda. Kui petturid aga ei tea sihtmärgi andmeid ning paroole, on mitmeid võimalusi nende saamiseks. (Dissecting wire fraud... 2013: 3) Järgnevalt esitatakse tabel 3, kus on esitatud peamised petturite meetodid isiklike andmete saamiseks ning nende meetodite kirjeldused.

Tabel 3. Petturite meetodid isiklike andmete saamiseks ülekandepettuste toime panemiseks ning nende kirjeldused

MEETOD	KIRJELDUS
Phishing	E-kiri, mis näeb välja nagu panga poolt saadetud, paludes ohvril kinnitata isiklikke või finantsandmeid.
Vishing/Smishing	*Vishingu* korral pettur helistab ohvrile, väites end olevat pank ning paludes, et kinnitatakse isiklik informatsioon telefoni teel. *Smishingu* korral aga ohver saab tekstisõnumi, kus on number millele tuleb helistada. Helistades numbrile, automaatvastaja küsib isiklikke andmeid.
E-posti ohtuseadmine	See töötab kahel viisil. Saades ligipääsu e-postile, võib viia internetipanganduse ligipääsuni ning vastupidi. Mõlemat pidi pettur saab ligipääsu mõlemale süsteemile. Pääsedes ligi e-posti kontole, on väga suur võimalus, et e-posti parool kattub või sarnaneb internetipanga paroolile. Lisaks saavad kurjategijad ligipääsu isiklikele andmetele, mida saab kasutada pangakonto ja internetiteenuste autentimisel.

Allikas: Autori koostatud Dissecting wire fraud... (2013: 3) põhjal.

Tänapäeval on petturitel muljetavaldavad oskused, et toime panna pettus (Fighting wire fraud...2013: 2). Tavaliselt ülekandepettuste toimepanemise skeemid jagunevad kolme põhirühma (Fighting wire fraud...2013: 2-3):

- skeem 1- „ma olen, kes ma ütlen, et olen“;
- skeem 2- „palun kinnitage oma informatsioon“;
- skeem 3- „sa oled ainuke, kes aidata saab“.

Skeem 1- Kurjategijatel on sageli olemas vajaminevad andmed, et võtta täielikult üle kliendi konto. Ülekande algatades on vajalik läbida „test“, kus pank kontrollib tehingu legitiimsust. Kui pank kontrollib ning peab kurjategija poolt pakutud andmeid õigeks, edastatakse ülekanne. (Fighting wire fraud...2013: 2)

Skeem 2- Kurjategijad on väga kogenud tehnoloogia kasutamises, et varastada või kavaldada isikuid isiklike andmete avaldamiseks (Fighting wire fraud...2013: 3). Eelnevalt on esitatud petturite meetodid (vt tabel 3), mis esindavad kõige sagedasemaid lähenemisviise, et koguda andmeid ülekandepettuse toimepanemiseks.

Skeem 3- Ohver saab e-posti teel kirja „sõbralt“ või „tuttavalt“, kes on hädas ning vajab raha. Kuna kiri on „sõbralt“ ning tunda on hädaolukorda, siis tehakse petturile pangaülekanne. (Fighting wire fraud...2013: 3)

On mitmeid pettuste skeeme ning nende taga on mitmed faktorid, mis ajendavad kurjategijaid pettustele. Tuntud teooria, mida on eriala kirjanduses palju arutatud, on pettuse kolmnurga teooria. See teooria määratleb elemente, mis viivad kurjategijad pettuse toimepanemiseni. (Ruankaew 2016: 474) Wolfe ja Hermanson (2004) lisasid aga pettuse kolmnurgale elemendi juurde ning lõid pettuse teemanti teooria. Autorid uskusid, et pettuse kolmnurk võiks parandada nii pettuse ennetamist kui ka avastamist juhul, kui lisada neljanda elemendi. Nimelt lisaks ajendile, võimalusele ning ratsionaalsusele, lisasid Wolfe ja Hermason elemendi, milleks on võimekus. (Wolfe, Hermanson 2004: 38) Seega peamised elemendid, mis viivad kurjategijad pettuste toimepanemiseni on (Wolfe, Hermason 2001: 39):

- ajend- soov või sund pettuse toimepanemiseks;
- võimalus- leidub süsteemis nõrkus, mida on võimalik kuritarvitada;
- ratsionaliseerimine- veendumus, et pettuslik tegevus on riski väärt;

- võimekus- on olemas tunnused ja võimed, et pettus toime panna.

On mitmeid pettuste skeeme, mille ohvriks on võimalik langeda. Selles alapeatükis tutvustati maksepettuseid ning kolme kõige levinumat maksevahendit, mida ohustavad kurjategijad. Samuti selgitati, millised tegurid ajendavad kurjategijaid pettustele. Järgmises alapeatükis esitatakse maksepettuste võimalikud tagajärjed ning tõkestamismeetmed.

1.2. Maksepettuste tõkestamise võimalused

Selles alapeatükis selgitatakse maksepettuste võimalike tõkestamismeetmeid, mis on pankade poolt kasutusele võetud. Samuti esitatakse majandusteadlaste arvamus maksepettuste tõkestamise kohta, esitatakse maksepettuste võimalikud tagajärjed ning selgitatakse kuidas on maksepettuseid käsitletud Eesti õigussüsteemis.

Pettus avaldab märkimisväärset mõju makseteenuste kasutajatele ning pankadele. Seetõttu on väga oluline, et meetmed oleksid tõhusad ning võimaldaksid pettuse ennetamist, avastamist ja pettuse vastu võitlemist. (Fraud prevention... 2011: 16)

Pettus avaldab negatiivset mõju pankadele ning panga klientidele, sest (Fraud prevention... 2011: 13):

- pettus võib suurendab kulutusi tarbijatele;
- tulemuseks on raskendatud juurdepääs teenustele tänu suurenenud turvameetmetele (näiteks ulatuslikum ID kontroll);
- pettus vähendab tarbijate usaldust panga poolt pakutavate toodete ja teenuste vastu;
- pettus kahjustab pankade mainet.

Majandusteadlased on peamiselt huvitatud kõige tõhusamast võimalikust maksesüsteemist. Mõned majandusteadlased näevad loomulikku rolli riigivõimul, kes saab aidata kontrollida maksesüsteemi pettuseid, näiteks erinevate regulatsioonidega. (Summers 2009: 17-18)

Majandusteadlaste peamised arvamused maksepettuste tõkestamisele on järgmised (Summers 2009: 17-18):

- Turvalisuse saavutamiseks on vajalik pidev tähelepanu.
- Turvalisuse saavutamine on väga kallis.
- Koostöö erinevate osapoolte vahel on väga oluline ning vajalik, et saavutada väärtuslike tulemusi.
- Pankade edu sõltub peamiselt usaldusest ja mainest.

Tänu võimalikele pettusest tulenevatele kahjudele, finantsinstitutsioonid pidevalt otsivad uusi tehnoloogiaid pettuste avastamiseks ning tõkestamiseks (Sakharova 2012: 227). Järgnevalt toob autor välja erinevad võimalikud meetmed maksepettuste tõkestamiseks töös käsitletavate maksevahendite lõikes. Esimesena on vaatluse all maksekaardipettuste tõkestamise võimalused.

Maksekaarditehingud erinevad nii kaardi tüübi poolest (krediitkaart või deebetkaart) kui ka vormi poolest (plastikkaart või mobiilne seade). Teine oluline eristav tegur on aga see, kas kaart on tehingu ajal füüsiliselt olemas või mitte. (Dhameja *et al.* 2013: 116) Esimesena on vaatluse all pettused müügikohas. Selliste tehingute korral saab kaupmees kontrollida makse kehtivust, tehes kindlaks kaardiomaniku identiteedi ja kaardi ehtsuse (Sakharova 2012: 232).

Kaardimaksete turvalisuse täiustamine on pangaautomaadi ja kaardimakseterminaliga seotud pettuste vähenemise peamiseks põhjuseks. Kõige olulisem täiendus oli ulatuslik EMV standardi kasutuselevõtt. (Card payments in Europe...2014: 36) EMV on ülemaailmne maksekaartide standard, mis põhineb kiibitehnoloogial ning loodi 1994. aastal Europay International SA, MaterCard ja Visa poolt. 2011. aasta alguses võeti ülemaailma kasutusele 1,2 miljardit EMV kaarti koos 18,7 miljoni EMV terminaliga. (King 2012: 2) Enne kiibitehnoloogia kasutuselevõttu Euroopas, kaardiomanike andmed olid magnetribal, mis asub kaardi tagaküljel. See tehnoloogia leiutati 1940ndatel aastatel ning on osutunud äärmiselt lihtsaks petturitele kloonida käepäraste seadmetega. (Froud 2015: 275) Kiibi eeliseks on see, et seda on oluliselt raskem võltsida kui magnetriba. Kiipkaardid on oluline tehnoloogiline lahendus pettuse vastu võitlemiseks ja järk järgult asendab magnetriba kogu Euroopas. (The payment system...2010: 57)

Maksekaardipettust on raskem sooritada, kui kaardimakseterminalid on kiibivõimalusega. Kaardil olev kiip teeb kindlaks kaardi ehtsuse ja PIN teeb kindlaks kaardiomaniku. (Sakharova 2012: 232) Kaardid koos EMV kiipidega kaitsevad isikuandmeid, luues ainulaadse turvakoodi iga tehingu jaoks. EMV kiipkaardid raskendavad klientide makseinformatsiooni varastamist kaardimakseterminalidest, aga need ei kaitse tarbijaid kaotatud/varastatud kaartide probleemi eest. Petturid saavad kasutada varastatud kaardinumbreid, et teha oste internetis. Paljud kauplused on alles üleminekul EMV makseterminalidele, seega tarbijad võivad märgada, et uutel kiipkaartidel on ka magnetriba. (Fraud remains...2016: 8) Peamine pettuse probleem on väljaspool Euroopat asuvates riikides, kus kiipkaardid ei ole levinud (Card payments in Europe...2014: 36).

Kiibi ja PIN kasutamine on tõestanud, et see vähendab varastatud/kaotatud kaartide ja võltsitud kaartide pettuseid. Kuid see ei ole kasulik e-kaubandustehingutes. (Sakharova 2012: 232) Turvalisuse tagamiseks on Europol julgustanud turge loobuma magnetribast ning liikuma kiibitehnoloogiale. Suur osa kaardiväljastajatest ei ole loobunud magnetribast, kuna kaarte, kus on ainult kiip, ei ole veel võimalik kasutada ülemaailmselt. (Card payments in Europe...2014: 37)

Olles tutvunud müügikohas toimuvate pettuste tõkestamisega, esitatakse järgnevalt e-kaubanduspettuste tõkestamismeetmed. E-kaubandustehingutes võivad olla mitmed tunnusmärgid, et tehing on seotud pettusega, näiteks esmakordne poodleja, ebatavalised ostukogused, kaubad kõrge edasimüügi väärtusega, mitmed tehingud sama kaardiga lühikese aja jooksul jne. (Sakharova 2012: 232)

2013. aasta jaanuaris avaldas Euroopa Keskpank kogumi *"Recommendations for the security of internet payments"*, eesmärgiga suurendada makseteenuse pakkujate järelvalveasutuste teadmisi, mis on seotud probleemidega elektrooliliste maksete ja instrumentide turvalisuses ning andes turvasoovitusi makseteks interneti teel. Peamiselt internetimaksetes tuleb andmeid kaitsta läbi tugeva tarbija autentimise, kindlustamaks, et tegemist ei ole petturiga kes algatab makset. Teine oluline soovitus on, et makseteenuste pakkujad peavad toimima nii, et ennetada, avastada ja tõkestada petturlikud maksetehingud. (Card payments in Europe... 2014: 36)

On mitmeid lahendusi, et kaitsta e-kaubanduse keskkonda. Üheks võimaluseks on panga kliendi käitumise analüüs. Selle korral pank jälgib kasutaja tehinguid teatud perioodi jooksul, et avastada kahtlaseid tegevusmustreid. (Conroy 2014: 8) Lisaks pettuse tõkestamiseks on kasutusel turvaelemendid CVV2/CVC2 (*Card Verification Value/Code*) ja AVS (*Address Verification Service*). AVS korral kontrollitakse kaardiomaniku maksmisaadressi, kuigi kui pettur teab ohvri aadressi, ei ole pettus välistatud. CVV2/CVC2 on aga kolme või nelja digitaalnumbriline kood maksekaardi peal. See aitab kontrollida, kas klient füüsiliselt omab kaarti tehingu ajal. (Sakharova 2012: 232) Samas, kui kaart on varastatud, ei aita turvaelemendid CVV2/CVC2 pettust vältida (Patidar, Sharma 2011: 33).

Lisaks esitatud võimalikele tõkestamismeetmetele, on uus kaitsemehhanism, et võidelda e-kaubanduspettuste vastu. Selleks on 3D turvasüsteem, nagu *Verified by Visa* ja *MasterCard SecureCode*. (Credit card fraud: How to...2009: 26) 3D turvasüsteem on protokoll, mille eesmärk on lisada täiendavaid turvakihte e-kaubandustehingute autentimisele (Conroy 2014: 9). *MasterCard SecureCode* ja *Verified by Visa* võimaldab kaardiomanikel kinnitada ennast läbi isiklike paroolide, mille nad loovad, kui registreerivad oma kaardi selle programmiga (Sakharova 2012: 232).

Pangad on kasutusele võtnud mitmeid tõkestamismeetmeid vältimaks kaardipettuseid. Sakharova on selgitanud, kes on peamiselt vastutav nii e-kaubanduspettuste kui ka müügikohas toimuvate pettuste korral. Selgus, et kaardipettused mõjutavad kõige vähem kaardiomanike ning peamine vastutus on pankadel. Kuna pettuste arv kasvab, on pangad sunnitud suurendama investeeringuid uude tehnoloogiasse, et kaitsta end kui ka oma kliente pettuste eest. (Sakharova 2012: 232)

Võib mõista, et välja on arendatud mitmeid turvameetmeid tõkestamaks kaardipettuseid. Samas maailm pidevalt areneb ning turule tuleb juurde uusi innovaatilisi maksevahendeid. Üheks võimalikuks maksevahendiks on multifunktsionaalsed kaardid, mis annavad kaardiomanikule ligipääsu mitmetele kontodele ühel plastikkaardil. Näiteks ligipääsu deebetkontole ja krediitkontole samal plastikkaardil ning võimaluse valida isikliku ja ettevõte konto vahel. (Christiansen 2011: 4) Lisaks üha enam tarbijaid on kasutusele võtnud mobiilimaksed (Christiansen 2011: 5). Christiansen (2011: 9) arvates on väga tõenäoline, et tulevikus kaarditurul ei eksisteeri füüsilisi kaarte.

Autori arvates erinevate maksevahenditega kaasnevad erinevad ohud. Turule tulevad uued maksevahendid, mida petturid üritavad ära kasutada, kuid pankadel tuleb kurjategijatest olla samm eespool ning igale uuele maksevahendile rakendada sobilike turvameetmeid.

Olles tutvunud maksekaardipettuste erinevate tõkestamisvõimalustega, esitatakse järgnevalt tšekipettuste tõkestamisvõimalused. Nagu oli näha alapeatükis 1.1, on mitmeid liike tšekipettuseid, mille ohvriks on võimalik langeda.

Pangad saavad kõige paremini kindlaks määrata, kas tšeki maksja allkiri ning tšeki saaja nimi on tšekil ehtsad (Sullivan 2014: 32). Samuti tšekipettuste vältimiseks on pankadel võimalik (Stop check fraud before...2001: 2):

- põhjalikult identifitseerida klienti;
- kontrollida kliendi allkirja;
- kontrollida kontojääki, et veenduda rahaliste vahendite olemasolus;
- Uurida kahtlaseid tšekke. Pankadel on õigus viivitada tšeki maksmisega, et kontrollida allkirja ja tšeki ehtsust.

Järgnevalt esitatakse ülekandepettuste võimalikud tõkestamismeetmed. Dhameja, Jacobs ja Porter on esitanud kolm üldist võimalust, kuidas pangad tõkestavad ülekandepettuseid (Dhameja *et al.* 2013: 112):

- klientide harimine ülekandepettuste ning andmete kaitsmise võimaluste kohta;
- internetipanga volitamata juurdepääsu järelvalve;
- luua ja hooldada protsesse ning meetmeid, et teha kindlaks ja peatada petturlikud tehingud.

Lisaks, pettuse tõkestamismeetmed tavaliselt keskenduvad ühele või mitmele järgmistest komponentidest (Fighting wire fraud...2013: 6-7):

- autentimise protsess,
- konto hooldamine,
- tehingute järelvalve ja autentimine.

Autentimise protsess hõlmab klientidelt kogutud andmete võrdlust konto avalmise ajal esitatud andmetega, nagu näiteks kasutajanimi, parool ning midagi, mida ainult kasutaja

teab (näiteks koera nimi). Täiendavad tegurid on näiteks kliendi arvutiseadme informatsioon, mida pank vaatleb ning seob kontoga. (Fighting wire fraud...2013: 6)

Järgmisena vaadeldakse konto hooldamise komponenti. Et avada uus konto, pank kogub andmeid, näiteks nimi, aadress, telefoninumber, emaili aadress, sünniaeg. Kui klient muudab oma andmeid, näiteks telefoninumbrit või emaili aadressi, kontakteerub pank kliendiga, veendumaks, et klient tegi tõesti muudatuse. (Fighting wire fraud...2013: 6)

Tehingute järelvalve ja autentimise korral tarkvara analüüsib klientide maksetegevust. Näiteks ülekande päring, et saata raha suure rahajäägiga kontole kuid väikese tehingute mahuga võib anda märku pettusest. Kui mistahes põhjusel pank kahtlustab, et ülekanne on petturlik, võib pank kontakteeruda kliendiga, et kinnitada taotlus. Tihtipeale võib klient, kellega ühendust võetakse, olla hoopis pettur, kes muutis kliendi andmeid, et sooritada pettus. (Fighting wire fraud...2013: 7)

Kui pettuse oht on tuvastatud, saab pank rakendada järgmiseid strateegiaid (Wire fraud prevention 2014: 1):

- Reaalajas nõuda kliendilt täiendavat autentimist, kuid ainult siis, kui algatatud ülekanne on ebatavaline kliendi kohta.
- Hoida makset kinni kuniks lõpliku pettuse analüütiku otsuseni.

Maksepettuste tõkestamiseks on rakendatud mitmeid meetmeid, kuid kui kurjategijad suudavad, vaatamata tõkestamismeetmetele, toime panna pettuse, ootab neid ees karistus. Eesti Karistusseadustikus vastavad maksepettustele viis paragrahvi. Paragrahvid ning nende sisu kirjeldused on esitatud tabelis 4.

Tabel 4. Karistusseadustikus maksepettustele vastavad paragrahvid Eestis

Paragrahv	Paragrahvi sisu
§ 199. Vargus	Võõra vallasasja äravõtmise eest selle ebaseadusliku omastamise eesmärgil – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
§ 213. Arvutikelmus	Varalise kasu saamise eest arvutiprogrammide või andmete sisestamise, vahetamise, kustutamise, sulustamise või muul viisil andmetöötlusprotsessi sekkumise teel, kui sellega on mõjutatud andmete töötlemise tulemust, - karistatakse rahalise karistuse või kuni viieaastase vangistusega.
§ 333. Maksevahendi ja väärtpaberi võltsimine	Raha, pangakaardi või muu maksevahendi, aktsia, obligatsiooni või muu väärtpaberi võltsimise eest kasutamise eesmärgil - karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
§ 334. Võltsitud maksevahendi ja väärtpaberi kasutamine	Võltsitud raha kasutamise, vahetamise, edasiandmise või muul viisil käibelelaskmise, samuti pangakaardi või muu võltsitud maksevahendi või väärtpaberi kasutamise eest - karistatakse rahalise karistuse või kuni viieaastase vangistusega.
§ 340. Raha, pangakaardi ja muu maksevahendi, väärtpaberi, maksumärgi, postimaksevahendi ja selle jäljendi ning proovijärelevalve märgistuse võltsimise ettevalmistamine	Raha, pangakaardi või muu maksevahendi, väärtpaberi, maksumärgi, postimaksevahendi või selle jäljendi või proovijärelevalve märgise võltsimiseks vajaliku seadeldise või muu vahendi soetamise, valmistamise, kohandamise, hoidmise või edasiandmise eest - karistatakse rahalise karistusega.

Allikas: Autori koostatud Karistusseadustik (2001) põhjal.

Ülaltoodud tabelis 4 on näha, et Eestis maksepettustega seotud kuritegude eest on karistuseks kas vangistus või rahaline karistus. Võib mõista, et tegemist on raske kuriteoga ning kuriteo toimepanemisel võib saada tugeva karistuse.

Selles alapeatükis vaadeldi maksepettuste võimalike tagajärgi ning tõkestamismeetmeid. Samuti esitati õiguslik pool, mis käsitleb maksepettuste eest saadavat karistust Eestis. Järgmises peatükis esitatakse maksepettused Eestis ning ühtses euromaksete piirkonnas. Samuti esitatakse küsitluste tulemused Eestis kasutatavate maksepettuste tõkestamismeetmete kohta.

2. MAKSEPETTUSTE LEVIK NING NENDE TÕKESTAMINE EESTIS

2.1. Maksepettuste levik Eestis

Selles alapeatükis on vaatluse all maksepettused Eestis. Esmalt vaadeldakse sularahata maksevahendite kasutamise rohkust Eestis, eesmärgiga välja selgitada, millist maksevahendit kasutatakse kõige rohkem. Kuna bakalaureusetöös on vaatluse all tšekid, pangaülekanded ning pangapoolsed maksekaardid, siis võrreldakse loetletud maksevahendite kasutamise rohkust. Lisaks esitatakse registreeritud maksepettustega seotud juhtumite arv Eestis perioodil 2013-2015. Samuti selles alapeatükis esitatakse maksekaardipettuste statistika ühtses euromaksete piirkonnas (SEPA alal) ning võrreldakse maksekaardipettuseid Eestis ning Eesti naabrriikides. Tulemused selgitavad, millist tehingukanalit peamiselt kasutatakse kaardipettuse toimepanemiseks Eestis ning SEPA alal. Lisaks selgitatakse välja maksepettuste eripära Eestis.

Bakalaureusetöös on vaatluse all sularahata maksevahenditest tšekid, kaardimaksed ning pangaülekanded ehk maksekorraldused. Kaardimaksed hõlmavad e-kaubanduse tehinguid ning kaardimakseid müügikohas (Mittefinantsettevõtete ja...(tükki) 2016). Järgnevalt esitatakse tabel 5, kus on sularahata makstavate maksete arv Eestis maksevahendite lõikes perioodil 2010-2015. Tabelis 5 on vaatluse all mittefinantsettevõtted ja kodumajapidamised ning väärtused tabelis on ümardatud.

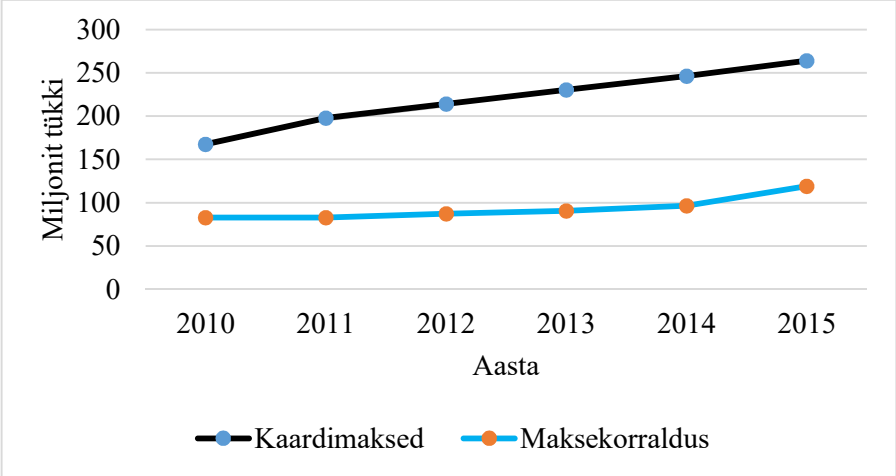
Tabel 5. Mittefinantsettevõtete ja kodumajapidamiste sularahata makstavate maksete arv Eestis makseviisi lõikes (miljonit tükki)

Makseviis	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Tšekid	0,000994	0,000527	0,002969	0,003626	0,003093	0,002822
Kaardimaksed	167,36	197,84	214,09	230,24	246,32	264,15
Maksekorraldus	82,70	82,96	87,20	90,76	96,42	118,98

Allikas: Autori kohandatud Mittefinantsettevõtete ja...(tükki) (2016) põhjal.

Ülaltoodud tabelist 5 on näha, et aastast aastasse on kõige rohkem vaatlusalustest sularahata maksevahenditest kasutusel kaardimaksed. Kaardimaksetele järgneb maksekorraldus ning kõige vähem kasutatakse maksevahendina tšekke. 2015. aastal kasutati tšekke vaid 2822 korral ning Euroopa Keskpanga (2007) kohaselt, tšekid ei ole maksevahendina omanud kunagi suurt rolli Eestis (Payment and securities... 2007: 103).

Kaardimaksed ning maksekorralduste kasutamine ületavad oluliselt tšekkide kasutamist. Järgnevalt võrreldakse kaardimaksete ja maksekorralduste kasutamise rohkust Eestis perioodil 2010-2015. Kui tšekkide kasutamine oli sadades ning paarituhandetes, siis kaardimaksed ja maksekorralduste kasutamise rohkus aastas on miljonites.



Joonis 1. Kaardimaksete ning maksekorralduse kasutamine Eestis miljonites tükkides perioodil 2010-2015 (autori koostatud mittefinantsettevõtete ja...(tükki) 2016 põhjal).

Jooniselt 1 on näha, et kaardimakseid on vahemikus 2010-2015 kasutatud rohkem kui maksekorraldust. Nii kaardimaksed kui ka maksekorraldus on alates 2010. aastast olnud kasvusuunas. Kaardimaksete kasutamise rohkus ületab 2012. aastal 200 miljoni piiri, kuid maksekorralduste kasutamine ületab 100 miljoni piiri alles 2015. aastal. 2015. aastal aga kasutati kaardimakseid 264,15 miljonil korral ning maksekorraldust 118,98 miljonil korral.

Tšekkide, maksekorralduse ning kaardimaksete kasutamise rohkus erinevad suuresti. Kasutamise rohkuse poolest on esikohal kaardimaksed, teisel kohal aga maksekorraldused, millele järgneb tšekkide kasutamine. Võib mõista, et Eestis pole tšekid levinud maksevahend. Järgnevalt võrreldakse sularahata makstavate maksete

käivet maksevahendite lõikes. Selleks on koostatud tabel 6, kus arvud on esitatud miljonites eurodes.

Tabel 6. Mittefinantsettevõtete ja kodumajapidamiste sularahata makstavate maksete käive Eestis makseviisi lõikes (miljonit eurot)

Makseviis	2010	2011	2012	2013	2014	2015
Tšekid	1,1	0,6	3,7	5,6	4	3,8
Kaardimaksed	2718,2	3161,6	3590,7	3954,5	4303,9	4692,1
Maksekorraldused	106 982,6	125 898,2	161 752,2	189 728,1	171 300	148 403,7

Allikas: Autori kohandatud Mittefinantsettevõtete ja...(miljon eurot) (2016) põhjal.

Tabelist 6 on näha, et tšekkide käive aastas on palju väiksem kui kaardimaksete ja maksekorralduste käive. Kõige suurem tšekkide käive oli 2013. aastal, nimelt 5,6 miljonit eurot, kuid peale seda hakkas käive langema. Kui kasutamise rohkuse korral domineeris kaardimaksed, siis vaadates tabelit 6, domineerib käibe poolest aga maksekorraldused.

Kaardimaksete käive perioodil 2010-2015 jääb alla 5000 miljoni euro. Tabelist 6 on näha, et kaardimaksete käive on kasvusuunas ning 2015. aastaks kasvas käive 4692,1 miljoni euroni. Maksekorralduste puhul aga perioodil 2010-2015 ületab käive 100 000 miljonit eurot. Maksekorralduste käive on alates 2010. aastast olnud kasvusuunas ning 2013. aastaks kasvas käive 189 728,1 miljoni euroni. Seejärel hakkas käive langema ning 2015. aastaks langes käive 148 403,7 miljoni euroni.

Seega kokkuvõtlikult võib öelda, et tšekkide kasutamine ei ole Eestis levinud. Kaardimaksed aga domineerivad kasutamise rohkuse poolest, kuid maksekorraldus ületab kaardimakseid käibe poolest. Seega, kaardimakseid kasutatakse Eestis rohkem, kuid maksekorralduste puhul on makse väärtus suurem.

Euroopa Liidus samuti kasutatakse vaatlusalustest maksevahenditest kõige rohkem maksekaarte, nimelt kaartitehingute arv kokku oli 2014. aastal 47,5 miljardit (Payment Statistics... 2015: 1). Ülekannete kasutamise rohkus oli 2014. aastal veidi üle 25 miljardi ning tšekkide kasutamise arv jäi alla 5 miljardi (Payment Statistics... 2015: 2).

Järgnevalt uuritakse maksepettuste levikut Eestis ning esimesena on vaatluse all tšekipettused ja ülekandepettused. Kuna konkreetset statistikat Eestis toime pandud ülekandepettuste ja tšekipettuste kohta pole kättesaadav informatsiooni

konfidentsiaalsuse tõttu, lähtub autor Eesti Karistusseadustikus maksepettustele vastavatest paragrahvidest ning registreeritud juhtumite arvust. Alapeatükis 1.2 esitati Eesti karistusseadustiku paragrahvid ning nende sisu kirjeldus (vt tabel 4), mis vastavad maksepettustele. Järgnevalt esitatakse tabel 7, kus on maksepettustele vastavad paragrahvid ning Eestis politsei poolt registreeritud maksepettusega seotud juhtumite arv aastatel 2013-2015.

Tabel 7. Maksepettustega seotud registreeritud juhtumite arv Eestis 2014. aastal

Paragrahv	**Registreeritud juhtumeid 2013. aastal**	**Registreeritud juhtumeid 2014. aastal**	**Registreeritud juhtumeid 2015. aastal**
§ 199. Vargus	16 465	15 738	11 354
§ 213. Arvutikelmus	470	486	494
§ 333. Maksevahendi ja väärtpaberi võltsimine	12	10	4
§ 334. Võltsitud maksevahendi ja väärtpaberi käitlemine	404	526	494
§ 340. Raha, pangakaardi ja muu maksevahendi, väärtpaberi, maksumärgi ning proovijärelevalve märgistuse võltsimise ettevalmistamine	11	12	-

Allikas: Autori koostatud Ahven *et al.* (2016: 98, 104) põhjal.

Tabelist 7 on näha, et Eestis esineb mitmeid maksevahenditega seotud kuritegevusi. Vaadates tabelis 4 esitatud paragrahvide sisu, arvab autor, et arvutikelmuse alla kuulub ülekandepettused. Arvutikelmuse registreeritud juhtumeid aastatel 2013-2015 oli vastavalt 470, 486 ja 494.

Autori arvates tšekipettused kuuluvad § 333, § 334 ning § 340 alla, sest alapeatükis 1.1 selgus, et üheks tšekipettuse liigiks on võltsitud tšekid. Loetletud paragrahvide registreeritud juhtumeid Eestis 2014. aastal oli vastavalt 10, 526 ning 12.

Kuna registreeritud juhtumid sisaldavad peale tšekkide ja ülekannete ka teisi maksevahenditega ja väärtpaberitega seotud pettuseid, siis ei ole võimalik konkreetselt

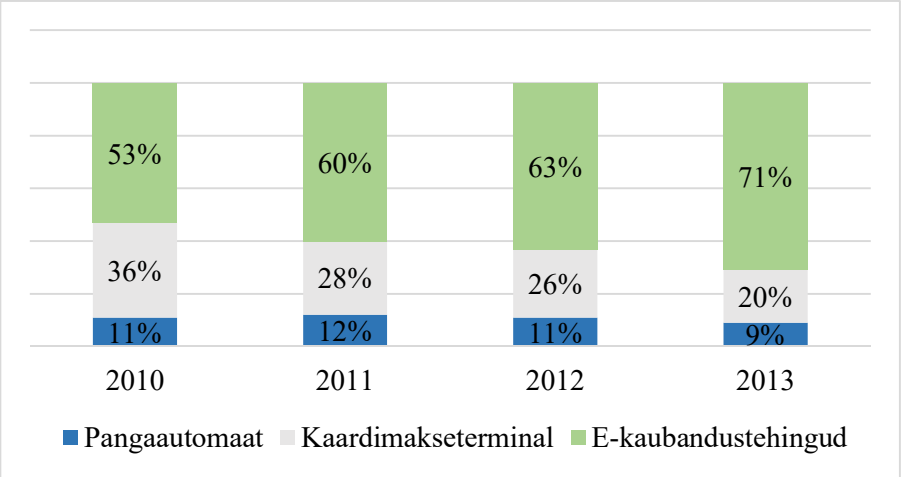
esitada tšekipettuste ning ülekandepettuste registreeritud juhtumite arvu Eestis. Kuid tabeli 7 põhjal võib mõista, et tšekipettuste ning ülekandepettuste arv Eestis on madal.

Bakalaureusetöös on peamine rõhk maksekaardipettustel. Nagu ka eelnevast analüüsist selgus, on maksekaardid Eestis peamine sularahata maksevahend. Järgnevalt vaadeldakse maksekaardipettusi SEPA alal.

Euroopa Keskpank on avaldanud aastatel 2012-2015 aruanded maksekaardipettuste kohta SEPA alal perioodil 2007-2013. SEPA on ühtne euromaksete piirkond kus on võimalik teha või vastu võtta euromakseid samades tingimustes sõltumata asukohast (Single Euro Payments Area 2016). Aruanded hõlmavad SEPA ala riike, kuhu kuuluvad Euroopa Liidu liikmesriigid ning Šveits, Island, Liechtenstein ja Norra (Report on card fraud 2012: 6; Second report on... 2013: 6; Third report on... 2014: 6; Fourth report on... 2015: 5).

SEPA alal väljastatud maksekaartide pettuse väärtus 2010. aastal oli 1,26 miljardit eurot (Report on card fraud 2012: 4), mis langes 2011. aastaks 1,16 miljardi euroni (Second report on... 2013: 4). 2012. aastaks kasvas kaardipettuste väärtus 1,33 miljardi euroni (Third report on... 2014: 4) ning 2013. aastaks 1,44 miljardi euroni (Fourth report on... 2015: 2).

Järgnevalt esitatakse joonis 2, kus on SEPA alal väljastatud kaartide pettused tehingukanalite lõikes perioodil 2010-2013. Joonis kirjeldab kaardipettuste erinevate tehingukanalite osatähtsust kõikidest kaardipettustest.



Joonis 2. Kaardipettuste osatähtsus tehingukanalite lõikes perioodil 2010-2013 (Fourth report on card fraud 2015: 8).

Ülaltoodud jooniselt 2 on näha, et perioodil 2010-2013 moodustas kõikidest kaardipettustest suurima osa e-kaubanduspettused. Sellele järgnes kaardimaksetерminalis toime pandud pettused ning viimasena pangaautomaatides toime pandud pettused.

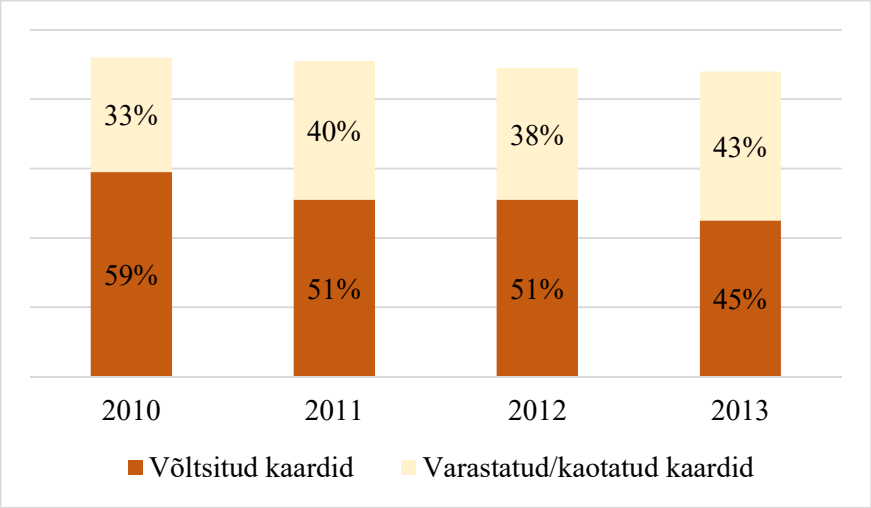
E-kaubanduspettused on alates 2010. aastast kasvusuunas ning 2013. aastaks moodustas 71% kõikidest kaardipettustest. Pettused kaardimaksetерminalis on alates 2010. aastast vähenenud ning 2013. aastal moodustas kõikidest kaardipettustest 20%. Pangaautomaadiga seotud pettused 2010. aastast kasvas ning moodustasid 2011. aastaks 12% kaardipettustest. Seejärel hakkas osatähtsus langema ning 2013. aastaks moodustas pettused pangaautomaatides 9% kõikidest kaardipettustest.

E-kaubanduspettuse väärtus oli 2010. aastal 648 miljonit eurot (Report on card fraud 2012: 4), 2011. aastal 655 miljonit eurot (Second report on... 2013: 4), 2012. aastal 794 miljonit eurot (Third report on... 2014: 4) ning 2013. aastal 958 miljonit eurot (Fourth report on... 2015: 2).

Nagu teoreetilises osas on öeldud, kaardimaksetерminali ning pangaautomaadi peamisteks pettuse liikideks on võltsitud kaardid ning varastatud/kaotatud kaardid. Need liigid moodustavad suurema osa kaardimaksetерminali ja pangaautomaadiga seotud pettustest.

Järgnevalt esitatakse joonis 3, kus on võltsitud kaartide ja varastatud/kaotatud kaartide osakaal kaardimaksetерminali ja pangaautomaadi pettustest protsentides. Vaatluse alt on

välja jäetud kaardipettuse liik, mille korral inimene pole pangakaarti kätte saanud, sest moodutab väga väikese osa pangaautomaadi ja kaardimaksеterminaliga seotud pettustest ning seda liiki pole käsitletud bakalaureusetöö teoreetilises osas.

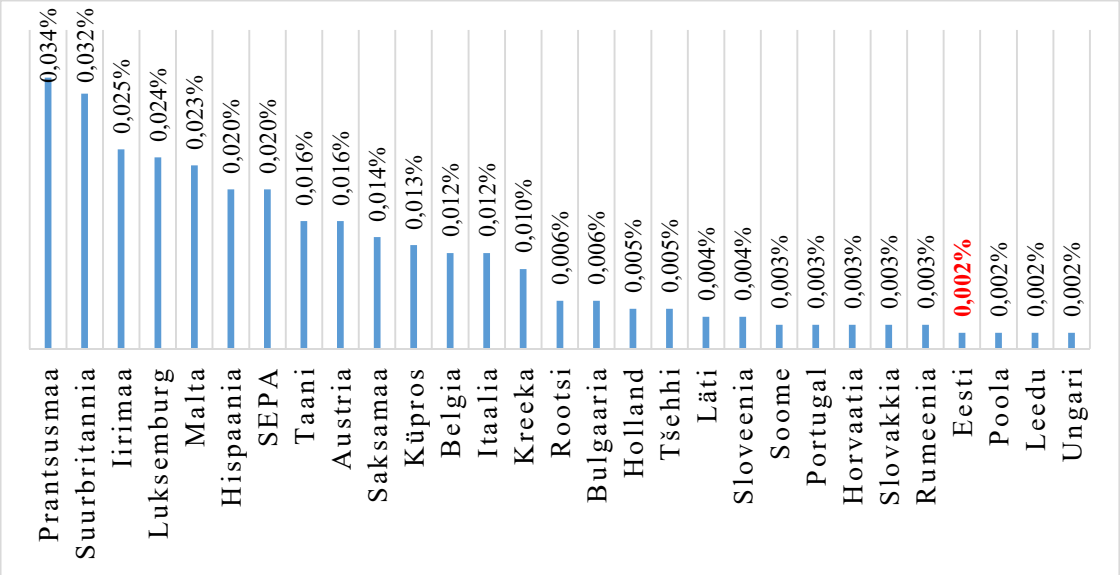


Joonis 3. Võltsitud ning varastatud/kaotatud kaartide pettuse osakaal kaardimaksеterminali ning pangaautomaadi pettustest SEPA alal perioodil 2010-2013 (Fourth report on card fraud 2015: 13).

Ülaltoodud jooniselt 3 on näha, et võltsitud kaartide osakaal on suurem kui varastatud/kaotatud kaartide osakaal. Võltsitud kaartide osakaal kaardimaksеterminali ja pangaautomaadi pettustest on kahanevas suunas ning 2013. aastaks moodustas see 45% pangaautomaadi ja kaardimaksеterminaliga seotud kaardipettustest. Varastatud/kaotatud kaartide osakaal alates 2012. aastast on vähenenud ning saavutas 2013. aastaks 43% pangaautomaadi ja kaardimaksеterminaliga seotud kaardipettustest. Nagu võib näha, 2010. aastal oli võltsitud kaartide osakaal varastatud/kaotatud kaartidest ligi 1,8 korda suurem, kuid 2013. aastaks on osakaalud ühtlustunud (vastavalt 45% ja 43%).

Euroopa Keskpanga poolt avaldatud aruande kohaselt, võltsitud kaartide pettused on oluliselt vähenenud ning see on tihedalt seotud sellega, et kaardimaksеterminalid ja kaardid mis on väljastatud Euroopas, vastavad EMV ehk ülemaailmse maksekaartide standarditele (Fourth report on card fraud 2015: 14).

Järgnevalt esitatakse joonis 4, kus on esitatud pettuse osatähtsus kaarditehingute arvust Euroopa Liidu liikmesriikide lõikes 2013. aastal. Joonis on esitatud kahanevas järjekorras.



Joonis 4. Pettuse osatähtsus kaarditehingute arvust Euroopa Liidu liikmesriikide lõikes 2013. aastal (autori koostatud Fourth report on card fraud 2015: 24 põhjal).

Ülaltoodud jooniselt 4 on näha, et Prantsusmaal on pettuse osatähtsus 0,034% ning see on SEPA alal ühtlasi kõige suurema pettuse osatähtsusega. Eesti asub joonisel aga tagapool, nimelt pettuse osatähtsus kaarditehingute arvust 2013. aastal oli vaid 0,002%. Eestis on pettuse osatähtsus väiksem kui naaberriik Soomes (0,003%), Lätis (0,004%) ning Rootsis (0,006%). Lisaks Eestile, on ka Poola, Leedu ning Ungari kõige väiksema pettuse osatähtsusega kaarditehingute arvust (0,002%).

Järgnevalt esitatakse kokkuvõtlik tabel 8 Eesti, Rootsi, Soome, Läti ning Leedu kohta. Esitatud on vaatlusalustes riikides pangakaarte elaniku kohta, tehinguid kaardi kohta ning pettusi 1000 kaardi kohta 2013. aastal.

Tabel 8. Pangakaarte elaniku, tehinguid kaardi ning pettusi 1000 kaardi kohta 2013. aastal Rootsis, Soomes, Eestis, Lätis ja Leedus (tükki)

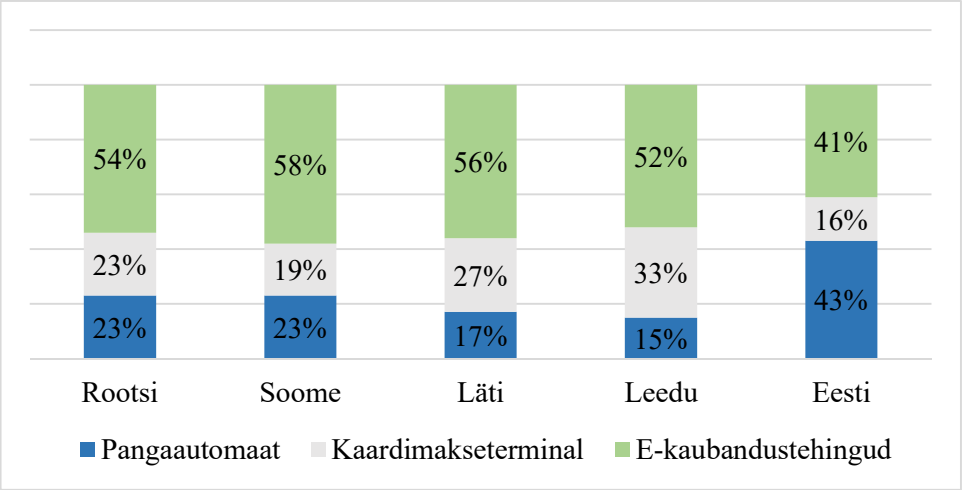
Riik	Pangakaarte elaniku kohta (tükki)	Tehinguid pangakaardi kohta (tükki)	Pettusi 1000 pangakaardi kohta (tükki)
Rootsi	2,3	112	6,8
Soome	1,4	166	6
Eesti	**1,3**	**149**	**3,5**
Läti	1,2	75	3
Leedu	1,2	61	1

Allikas: Autori koostatud Fourth report on card fraud (2015: 24) põhjal.

Tabelist 8 on näha, et Eestis on 2013. aastal pangakaarte elaniku kohta 1,3 ning edastab sellega Lätit ja Leedut, kus pangakaarte elaniku kohta on 1,2. Eestit edastab Soome, kus pangakaarte elaniku kohta on 1,4 ning Rootsi, kus on 2,3 pangakaarti elaniku kohta. Tabelist on näha, et Soomes on kõige rohkem tehinguid pangakaardi kohta (166), millele järgneb Eesti (149), Rootsi (112), Läti (75) ning viimasena Leedu (61). Huvitav on asjaolu, et Eestis on tehinguid pangakaardi kohta rohkem kui Rootsis (vastavalt 149 ja 112 tehingut pangakaardi kohta), kuigi Rootsis on pangakaarte elaniku kohta (2,3) rohkem kui Eestis (1,3). Lisaks, Eestis on umbes 1,9 korda vähem pettusi 1000 pangakaardi kohta kui Rootsis (vastavalt 3,5 ja 6,8 pettust 1000 pangakaardi kohta)

Võrreldes aga Lätiga, on Eestis ligi kaks korda rohkem tehinguid pangakaardi kohta ning vaid 1,2 korda rohkem pettusi 1000 kaardi kohta. Näiteks Leedus on aga vähe tehinguid kaardi kohta (61) ning samuti pettusi 1000 kaardi kohta vähe (üks). Võib mõista, et Eesti eristub teistest riikidest kõrge tehingute arvu kuid väikese pettuste arvu poolest.

Järgnevalt vaadeldakse kaardipettuse osatähtsust tehingukanalite lõikes vaatlusalustes riikides 2013. aastal. Selleks on koostatud joonis 5.

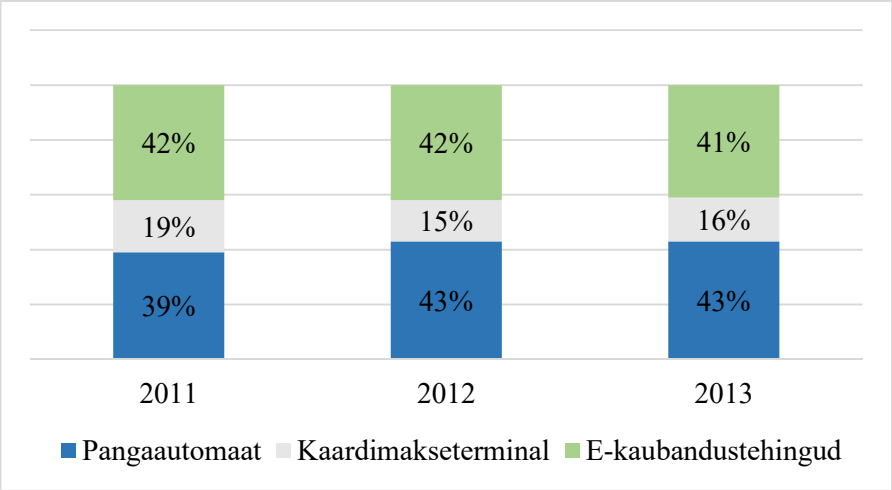


Joonis 5. Pettuse osatähtsus tehingukanalite lõikes 2013. aastal Rootsis, Soomes, Lätis, Leedus ja Eestis (autori kohandatud Fourth report on card fraud 2015: 22 põhjal).

Jooniselt 5 on näha, et taaskord eristub Eesti teistest riikidest, nimelt kõige suurema osatähtsusega on kaardipettused pangaautomaatides (43%) kõikidest pettuse juhtumitest. Rootsis, Soomes, Lätis, Leedus on aga suurima osatähtsusega e-kaubanduspettused.

Eestis on 2013. aastal pettuse osatähtsus kaardimaksеterminalis väikseim (16%), aga Lätis ja Leedus on väikseima osatähtsusega just pettused sularahaautomaatides (vastavalt 17% ja 15%). Soomes on esikohal e-kaubanduspettused (58%), millele järgneb pettused sularahaautomaadis (23%) ning seejärel pettused kaardimaksеterminalides (19%). Rootsis aga on pettuste osatähtsus sularahaautomaadis ja kaardimaksеterminalis sama (23%).

Järgnevalt on vaatluse all pettuse osatähtsus Eestis tehingukanalite lõikes perioodil 2011-2013. Selleks on autor koostanud joonise 6.



Joonis 6. Pettuse osatähtsus Eestis tehingukanalite lõikes perioodil 2011-2013. (autori koostatud Second report on... 2013: 17; Third report on... 2014: 17; Fourth report on... 2015: 22 põhjal).

Jooniselt 6 on näha, et 2011. aastal oli Eestis väljastatud kaartidega enim e-kaubanduspettusi (42%). 2012. aastaks aga edastab e-kaubanduspettuseid pettused pangaautomaatides (43%). Perioodil 2011-2013 on kõige väiksema osatähtsusega pettused kaardimaksеterminalides kõikidest pettuse juhtumitest (vastavalt 19%, 15% ning 16%).

Huvitav on asjaolu, et 2013. aastal oli Eesti ainuke Euroopa Liidu liikmesriik, kus peamiseks pettuse tehingukanaliks oli pangaautomaat. Ülejäänud riikides oli peamiseks pettuse kanaliks e-kaubandus. (Fourth report on... 2015: 22)

Selles alapeatükis vaadeldi sularahata maksevahendite kasutusrohkust Eestis. Selgus, et Eestis on peamiseks sularahata maksevahendiks kaardimaksed, millele järgnevad maksekorraldus ning tšekid. Lisaks esitati maksepettuste statistika Eestis ning kaardipettuste statistika SEPA alal. Kaardipettustes Eesti eristub Rootsist, Soomest, Lätist ja Leedust suuresti. Nimelt, Eestis on suur tehingute arv kuid väike pettuste arv kaardi kohta. Lisaks pettuse osatähtsus pangaautomaatides on suurim, kuid teistes vaatlusalustes riikides on e-kaubanduspettuste osatähtsus kõikidest kaardipettustest suurim. 2013. aastal oli Eesti ainuke Euroopa Liidu liikmesriik, kus peamiseks pettuse tehingukanaliks oli pangaautomaat. Võrreldes Eestit teiste Euroopa Liidu liikmesriikidega, on Eestis pettuse osatähtsus kaarditehingute arvust väike (0,002%) ning

asub 2013. aastal koos Poola, Leedu ning Ungariga väikseima pettuse osatähtsusega riikide seas. Samuti Eestis on tšekipettuste ning ülekandepettuste arv madal ning kokkuvõtlikult võib öelda, et Eestis ei kujuta maksepettused suurt ohtu.

Järgmises alapeatükis esitatakse küsitluste tulemused maksepettuste kohta. Küsitluste tulemused aitavad välja selgitada Eestis kasutusel olevad maksepettuste tõkestamismeetmed.

2.2. Maksepettuste tõkestamine Eestis

Selles alapeatükis esitatakse autori poolt esitatud küsimuste tulemused maksepettuste kohta. Lisaks esitatakse järeldused ning autoripoolsed soovitused maksepettuste vähendamiseks.

Uurimaks Eestis kasutusel olevaid maksepettuste tõkestamismeetmeid, koostas autor varasemate uuringute põhjal küsimustiku, mis koosnes 12 küsimusest (vt lisa 1). Autor võttis ühendust Eesti Pangaliiduga, et saada maksepettuste tõkestamise valdkonnaga tegelevate isikute kontaktandmeid, kuna kontaktandmed pole avalikult kättesaadavad. Spetsialistide poole oli võimalik pöörduda vaid e-posti teel mis võib oluliselt vähendada tagasiside saamist. Autoriga koostööks oli valmis neli inimest.

Kolm vastajat tegutsevad Eesti kommertspankades ning üks vastaja tegutseb Eesti Pangas. Võttes arvesse vastajate anonüümsussoovi, tähistatakse vastajad X1, X2, X3 ja X4. Vastused on olnud kontaktisikute isiklikud seisukohad. X1 oli võimalik läbi viia intervjuu, mis toimus 23. märtsil 2016. aastal ning intervjuu kestuseks oli 40 minutit. Intervjueeritava nõusolekul intervjuu salvestati. X2, X3 ning X4 soovisid vastata küsimustele e-posti teel. Kõikide vastajate otseseks tegevusvaldkonnaks on maksekaardid, kuid X1 ning X3 on tegelenud ka tšekkide ning internetipanganduse valdkonnaga.

Bakalaureusetöö autori arvates on nelja inimesed vastused piisavad analüüsiks, kuna vastused on Eesti Panga ning Eesti kommertspankade antud valdkonnaga tegelevate spetsialistide poolt. Lisaks Eesti Pangaliidust öeldi, et tegemist on väga tundliku teemaga ning seda märkisid ka osad inimesed, kelle poole autor pöördus. Nimelt, Danskebank

polnud valmis koostööd tegema, põhjendades, et tegemist on konfidentsiaalse teemaga ning selle kohta väljaspoole infot ei anta. Lisaks mitmed märkisid, et konkreetset statistikat ei ole võimalik avaldada ning osadele küsimustele ei ole võimalik vastata. Autor arvestas teema riskantsusega kogu bakalaureusetöö vältel, kuid nelja spetsialisti vastused on piisavad välja selgitamaks Eestis kasutusel olevad maksepettuste tõkestamismeetmed.

Esmalt uuriti tšekkide kohta ning selleks esitati kaks küsimust. Küsimustele oskasid vastata X1, X3 ning ühele küsimusele ka X4. X2 ei saanud küsimusele vastata, kuna antud teema ei kuulu tema valdkonda. Järgnevalt esitatakse tabel 9, kus on kokkuvõtlikult esitatud küsimused ning saadud vastused tšekkide ning tšekipettuste kohta.

Tabel 9. Küsimused ning vastused tšekipettuste kohta

	X1	X3	X4
Miks Eestis ei ole tšekkide maksevahend levinud?	Pole mugav maksevahend. Eestis pole kunagi populaarne olnud.	Tšekkidest loobumine on seotud otstarbekusega.	Eestis jäi tšekkide kasutus arenguetapina vahele.
Millised on Eestis kasutusel olevad meetmed, et vältida tšekipettuseid?	Ranged reeglid. Allkirja kontrollimine, kliendi identifitseerimine	Pank, kus tegutsen, ei tee tehinguid tšekkidega.	-

Allikas: Autori koostatud küsitletute vastuste põhjal.

Uurides, miks Eestis ei ole tšekkide maksevahend levinud, erinesid vastajate arvamused. X1 arvamuse kohaselt tšekkide kasutamine ei ole mugav ning Eestis pole see maksevahend olnud kunagi populaarne (X1 2016, vt lisa 2). X3 hinnangul aga on tšekkidest loobumine seotud otstarbekusega ning selgitas oma argumenti järgmiselt (X3 2016, vt lisa 4):

„Tšekkidest loobumine on minu hinnangul seotud otstarbekusega. Kui on olemas finantssüsteem, mis katab ära tšekkidega seotud vajadused, siis need heidetakse kõrvale. Pankadele on tšekkidega seonduv liiga suur kuluartikkel ning kui välist surved antud teenusele ei ole, siis pole asjakohane pidada üleval tervet osakonda.“ (X3 2016, vt lisa 4)

Kolmas hinnang on vastaja X4 poolt ning vastaja esitas enda arvamuse, miks tšekid pole Eestis levinud maksevahend, nimelt (X4 2016, vt lisa 5):

„Ma usun, et peamine põhjus on selles, et pangandusvaldkonnas tegi kaardimakse areng suuri edusamme just ajal, mil tšekkide periood ei olnud veel jõudnudki oluliseks kasvada. Teisisõnu, Eestis jäi tšekkide kui makseviisi kasutus arenguetapina lihtsalt vahele. Teistpidi võiks öelda, et elektrooniliste kanalite areng oli piisavalt kiire ja nö peberil toimivad, aeglased ja tülikad tšekid ei tundunud atraktiivsed. Põhimõtteliselt võib öelda, et oli see turu loomulik ja väga positiivne areng, kuid ilmselgelt aitasid sellele kaasa ikka pangad krediitkaartide pakkumisega! Lõuna Euroopas, nt Prantsusmaal seevastu on tšekkidega arveldamist veel väga palju ja neil ei õnnestu omal ajal juurdunud harjumusest kuidagi lahti saada.“ (X4 2016, vt lisa 5)

Eelmises alapeatükis 2.1 oli näha, et tšekkide kasutamine pole Eestis levinud ning kasutusrohkus jääb suuresti alla maksekaartide ning maksekorralduste kasutamisele. Kuid vaatamata sellele, tehakse Eestis siiski tšekimakseid ning on vaja arvestada asjaoluga, et ka seda maksevahendit võivad ohustada kurjategijad. Seega autor uuris, millised on Eestis kasutusel olevad meetmed, et vältida tšekipettuseid. Pank, kus vastaja X3 tegutseb, ei tee tehinguid tšekkidega ning seega tšekipettustes ei ole võimalik panka ära kasutada (X3 2016, vt lisa 4). X1 vastuse kohaselt need pangad, mis võtavad vastu tšekke, läbivad rangeid kontrolle, näiteks allkirja kontrollimine, kliendi identifitseerimine ning muid protsesse, sest pettuse risk siiski esineb (X1 2016, vt lisa 2). Teoreetilises osas on samuti esitatud, et tšekipettuste vältimiseks pangad põhjalikult identifitseerivad klienti, kontrollitakse allkirja ning uuritakse tšekke, et avastada võimalikud võltsingud.

Võib mõista, et vaatamata vähesele tšekkide kasutamisele, on Eestis arvestatud pettuse ohuga ning kasutusel on karmid meetmeid, vältimaks tšekipettuseid. Järgnevalt esitas autor kaks küsimust ülekandepettuste kohta. Vastata oskasid vastajad X1 ning X3. Küsimused ja vastused ülekandepettuste kohta on kokkuvõtlikult esitatud tabelis 10.

Tabel 10. Küsimused ning vastused ülekandepettuste kohta

	X1	X3
Kuidas hindate ülekandepettuseid Eestis ning millised on tüüpilisemad näited?	Ülekandepettuse vähene levik Eestis. Peamine surve paroolikaartidele. Peamiselt *vishing*.	Paroolide vargus.
Millised on peamised ülekandepettuste tõkestamismeetmed?	Määratud on maksimaalne tehingu summa, mida saab teostada paroolikaardiga.	Laekumiste monitooring. Oluline on info kiire saabumine pettustest.

Allikas: Autori koostatud küsitletute vastuste põhjal.

Ülaltoodud tabelist 10 on näha, et vastajate X1 ja X3 arvates on ülekandepettused Eestis peamiselt seotud paroolide vargusega. X1 kohaselt, peamine surve kurjategijate poolt on paroolikaartidele ning levinud on *vishing* (X1 2016, vt lisa 2). Bakalaureusetöö teoreetilises osas on samuti märgitud, et see on peamine viis koos *phishingu* ja *smishinguga*, et koguda ohvritelt isiklike andmeid.

Tõkestamise poolepealt vastajate arvamused lahknesid. Nimelt X3 hinnangul peamiseks meetmeteks on klientide laekumiste monitooring (X3 2016, vt lisa 4). Seda on ka märgitud bakalaureusetöö teoreetilises osas, et ülekandepettuste tõkestamise võimaluseks on klientide maksetegevuse jälgimine. X1 väitis aga, et Eestis on määratud maksimaalne tehingu summa, mida saab teostada paroolikaardiga. Suuremate summade ülekandeks on vajalik ID kaart. Seega ülekandepettused pole atraktiivne vahend kurjategijatele ning ka see on üheks põhjuseks, miks ei ole Eestis ülekandepettused levinud. (X1 2016, vt lisa 2)

Alapeatükist 2.1 võis mõista, et tšekipettuste ning ülekandepettuste oht on Eestis väike. Kuid võib mõista, et Eestis esineb tšekipettuseid ja ülekandepettuseid ning nende tõkestamiseks on pangad rakendanud erinevaid meetmeid. Tšekipettuste tõkestamiseks kontrollib pank tšekil esitatud allkirja ehtsust ning tugevalt identifitseeritakse klienti. Ülekandepettuste tõkestamiseks aga pangad monitoorivad laekumisi ning Eestis on kehtestatud tehingu limiidid, mida on võimalik teostada paroolikaardiga.

Autori arvates tšekipettuste väike toimepanemise arv on seotud sellega, et Eestis ei ole tšekid levinud maksevahend ning Eestis mõned pangad ei tee tehinguid tšekkidega. Samuti Eestis on ranged tšekkide kontrollmeetmed ning see võib olla üheks põhjuseks,

miks tšekipettuste arv on väike. Autor soovitab pankadel harida kliente tšekipettuste kohta, näiteks selgitades, millised näevad välja pettuslikud tšekid.

Ülekandepettuste vähesus on autori arvates seotud sellega, et suuremate summade ülekandmiseks on vajalik ID kaart. Seega üheks põhjuseks, miks Eestis ei ole ülekandepettuste oht suur, on tugevad pettuste tõkestamismeetmed. Autor soovitab pankadel loobuda paroolikaartide väljastamisest ning nõuda tehingute teostamist vaid ID kaardi alusel. Samuti soovitab autor pankadel harida kliente *phishingu*, *smishingu* ning *vishingu* kohta. Pank küll võib tagada tugevad nõuded ning erinevate paroolide kehtestamise, kuid kui ohver annab kurjategijatel vajalikud andmed, ei aita turvameetmed pettust vältida.

Bakalaureusetöös on peamine rõhk kaardipettustel ning selle kohta esitas autor kaheksa küsimust. Autor on koostanud tabeli 11, kus on kokkuvõtlikult küsimused ja vastused kaardipettuste kohta. Vastajaid oli kokku neli, kuid osadele küsimustele X2 ei vastanud ning vastuseta kohta on tabelisse märgitud „-„ märk.

Tabel 11. Küsimused ja vastused kaardipettuste kohta

	X1	X2	X3	X4
Kuidas hindate maksekaardipettuste levikut Eestis?	Madal kaardipettuste risk.	Viimaste aegade mahutrendis suuri hüppeid ei ole.	Kaardipettuste arv on olnud tõusutrendis.	Kaardipettuste arv väike.
Millised on peamised kasutusel olevad kaardipettuste tõkestamismeetmed?	Üleminek magnetribalt kiibi kasutamisele. 3D turvasüsteem.	Kiipkaardid. Turvaelemendid kaartidel. 3D turvasüsteem.	Laekumiste monitooring.	Kiibitehnoloogia. 3D turvasüsteem.
Kas kasutusel olevad tõkestamismeetmed on piisavad pettuste tõkestamiseks?	Eksisteerib nõrki kohti, mida on võimalik ära kasutada.	-	Tõhusad piiratud ulatuses.	Pangad töötavad selle nimel, et muuta kaardid ja makselahendused turvalisemaks. Suur roll kaardi valdajal.
Millised on maksekaardipettuste tüüpilisemad näited Eestis?	E-kaubanduspettused.	-	Pettused pangaautomaadis (*skimming*).	Kaardilt andmete kopeerimine ja kaardi võltsimine.
Millised on maksekaardipettuste peamised põhjused?	Süsteemi keerukus.	-	Süsteemi nõrkused.	Ebaseadusliku kasu saamine.
Millised on peamised soovitused, et mitte langeda kaardipettuse ohvriks?	Kliendi tähelepanelikkus. Ei tohi jagada andmeid.	Klindil oluline olla teadlik ja mitte luua ülearuseid riskiolukordi.	Ei tohi jagada paroole ning andmeid teistele isikutele.	Üle vaadata pangakaardi kasutuslimiiti.
Kuhu tuleks pöörduda kui on langetud pettuse ohvriks?	Teavitada panka.	-	Teavitada panka ning Politsei- ja Piirivalveametit.	Ühendust võtma oma pangaga.
Kas kaardipettuste eripäral on seos tõkestamismeetmetega?	Jah.	-	Jah.	Jah.

Allikas: Autori koostatud küsitletute X1, X2, X3, X4 vastuste põhjal.

Esimesena uuriti kaardipettuste levikut Eestis ning selle muutumist viimase viie aasta jooksul. X3 hinnangul, pettuste arv on pigem tõusnud ning põhjendas oma argumenti järgmiselt (X3 2016, vt lisa 4):

„Kaardipettuste arv on viimastel aastatel olnud isikliku hinnangu kohaselt tõusutrendis. Turule on tulnud rida instrumente, mis on loonud soodsa pinnase kõikvõimalike maksepettuste läbiviimiseks.“ (X3 2016, vt lisa 4)

Vastukaaluks X3 arvamusele, X2 hinnangul viimastel aegadel suuri muutusi kaardipettustes ei ole olnud (X2 2016, vt lisa 3). Vastajate X1 ning X4 arvamused kattusid, nimelt Eestis on kaardipettuste arv väike (X1, X4 2016, vt lisa 2 ja 5). Enamasti mida rohkem kaarte kasutatakse, seda rohkem on ka pettuseid ning X1 tõi näiteks Prantsusmaa, kus maksekaardi kasutamisrohkus ning samuti ka kaardipettuste arv on suur. Leedus aga kaardimaksed pole levinud ning on ka kaardipettuseid vähem. (X1 2016, vt lisa 2)

Alapeatükis 2.1 selgus, et Prantsusmaa, võrreldes teiste Euroopa Liidu riikidega, on kõige suurema pettuste osakaaluga. Samuti oli näha, et Leedus on väike kaarditehingute ning kaardipettuste arv. Intervjueeritav X1 lisas, et Eesti on unikaalne piirkond, kus kaardimaksed on laialdaselt levinud, aga pettuseid on vähe (X1 2016, vt lisa 2). Autor märkis seda ka alapeatükis 2.1, kus statistikast oli näha, et Eesti eristub teistest riikidest kõrge kaarditehingute arvu, kuid väheste kaardipettuste poolest.

Järgmisena uuriti, millised on peamised kasutusel olevad kaardipettuste tõkestamismeetmed Eestis ning esimesena on vaatluse all müügikohas toimuvate pettuste tõkestamine. Vastajad X1, X2 ja X4 üheselt väitsid, et peamine meede kaardipettuste tõkestamiseks on olnud üleminek magnetribalt kiibitehnoloogiale (X1, X2, X4 2016, vt lisa 2, 3, 5). X3 aga ei esitanud müügikohas toimuvate pettuste tõkestamismeetmeid. Vastaja X4 selgitas kaardipettuste tõkestamist järgmiselt (X4 2016, vt lisa 5):

„Kaardipettus on enamasti rahvusvaheliselt organiseeritud tegevus, mille tõkestamine eeldab üleeuroopalist koostööd ning ennetavate meetmete ja rahvusvaheliste standardite kasutuselevõtmist. Kaardipettuste tõkestamiseks on keskpangad, pangad ja kaardiskeemid teinud juba märkimisväärseid jõupingutusi ning võtnud kasutusele

lisameetmeid, et muuta kaardimaksed turvalisemaks. Ühtses euromaksete piirkonnas vahetatakse magnetribad sujuvalt välja turvalisema kiibitehnoloogia vastu, mis vähendab kaardipettusi ja kaartide kopeerimist.“ (X4 2016, vt lisa 5)

Vastaja X2 andis põhjaliku hinnangu kiibitehnoloogiale (X2 2016, vt lisa 3):

„Pangakaartide valdkonnas (kus mina toimetan) on kiipkaardile üleminekuga toimunud oluline hüpe turvalisuse kasvus, sisuliselt ei ole kiipi võimalik murda. Samuti toimub pidev kiibi põlvkondade uuendamine ja kaasajastamine. Euroopa on juba ammu kiibile üle läinud, kuid Ameerikas on alanud ning Aasias käimas juba mõnda aega. Kuna nendes regioonides on prevaleeriv magnetriba kasutamine, siis näeme jätkuvalt just sealtpoolt rohkem väärkasutamist. Selles olukorras keskenduvad petturite ründed rohkem just magnetriba tehnoloogiale, mis on kopeeritav ning taaskasutav.“ (X2 2016, vt lisa 3)

Samuti X1 väitis, et kiipi on juba kolm korda tugevalt muudetud, kuid magnetriba pole kümnete aastate jooksul muudetud. Magnetriba kopeerimiseks on võimalik soetada väga odava hinna eest seade, millega on võimalik kopeerida andmeid. (X1 2016, vt lisa 2) X2 lisas, et kaardil on turvaelemendid, mis on väga olulised meetmed pettuste tõkestamiseks. (X2 2016, vt lisa 3)

Teoreetilises osas on märgitud, et tänapäeval on peamine müügikohas toimuvate pettuste tõkestamismeetmeks kiip, mis on oluliselt suurendanud turvalisust. Järgnevalt on vaatluse all küsitletute vastused e-kaubanduspettuste tõkestamisele. Vastajad X1, X2 ja X4 üheselt väitsid, et peamiseks tõkestamismeetmeks on 3D turvasüsteemi kasutuselevõtt. X3 hinnangul aga peamiseks meetmeks on laekumiste monitooring. Nimelt (X3 2016, vt lisa 4):

„Riske vähendavateks meetmeteks on monitoorida laekumisi. Monitooringu käigus võib selguda, et antud isikute tehingud ei ole läbipaistvad ja isik võib panna toime pettuse.“ (X3 2016, vt lisa 4)

X1 lisas, et algselt oli peamiseks pettuse tõkestamismeetmeks kaardinumber ja aegumiskuupäev, mille tuleb sisestada ostu sooritamiseks. Seejärel tuli välja turvaelemet CVV2/CVC2, mis oli suureks sammuks edasi. Tänapäeval on peamiseks tõkestamismeetmeks 3D turvasüsteem, mille korral on kaupmees süsteemist välja viidud

ning kaardiomanik autendib end täiendava parooliga. 3D turvasüsteemiga välditakse mitmeid riske, nimelt kui tegemist ei ole 3D turvasüsteemiga (nt tehingud CVV2/CVC2 alusel), on kaupmehele andmed kättesaadavad, mis on kurjategijatele atraktiivne siht, et süsteemi sisse murda. (X1 2016, vt lisa 2)

Bakalaureusetöö teoreetilises osas on märgitud, et üheks pangapoolseks e-kaubanduspettuse tõkestamismeetmeks on kliendi käitumise analüüs, mille korral jälgitakse kasutaja tehinguid. Samuti on märgitud, et turvaelemendid CVV2/CVC2 ning 3D turvasüsteem on peamised panga poolt kasutusele võetud meetmed kaardipettuste tõkestamiseks.

Võib mõista, et maksekaardipettuste tõkestamiseks on mitmeid meetmeid, kuid sellest tuleneb küsimus, kas need on piisavad pettuste tõkestamiseks. Seega autor esitas järgmise küsimuse, et teada saada, kas kasutusel olevad tõkestamismeetmed on piisavad pettuste tõkestamiseks. Vastaja X3 arvamuse kohtaselt (X3 2016, vt lisa 4):

„Kasutusel olevad meetmed on tõhusad üksnes piiratud ulatuses ja need peavad jätkuvalt astuma turul olevate finantstoodetega ühte sammu.

Kui ka meetmed oleks väga tõhusad, siis ei oleks see absoluutne. Edukas pettuse tõkestamine on enamasti seotud kiire reageerimisega petta saanud isiku poolt. Kui krediidiasutusele infot pettuse kohta ei laeku, siis ei pruugi kahjuks ka pank pettuse toimepanemisest teada. Seega ei ole tõhusust võimalik alati mõõta pankade poolt kehtestatud meetmetega.“(X3 2016, vt lisa 4)

X1 hinnangul leidub süsteemis nõrki kohti, näiteks magnetriba mida on võimalik kuritarvitada (X1 2016, vt lisa 2). Vastaja X4 kohaselt töötatakse selle nimel, et muuta kaardid turvalisemaks (X4 2016, vt lisa 5):

„Eesti pangad suurendavad pidevalt pangaautomaatide turvalisust, lisades pangakaardi võltsimise ja kopeerimise vastaseid seadmeid (nn anti-skimmer'eid), kuid täielikku kaitset ei taga ükski turvalahendus ega anti-skimmer.“ (X4 2016, vt lisa 5)

Seega võib öelda, et müügikohtades toimuvate kaardipettuste peamiseks tõkestamismeetmeks Eestis on kiipkaardid ning see on tänapäeval väga turvaline

lahendus, sest kiipi on pea võimatu murda. Peamiseks puuduseks on aga magnetriba, mis veel eksisteerib Eestis olevatel pangakaartidel. Magnetriba on lihtne kopeerida odavate seadmetega ning see on peamine nõrk koht.

E-kaubanduspettuste peamiseks tõkestamismeetmeks Eestis on 3D turvasüsteem, mille suur eelis on, et kaupmees on süsteemist välja viidud ning autentimine käib läbi isiklike paroolide. Puuduseks on aga see, et tehinguid teostatakse ka CVV2/CVC2 ning aegumiskuupäeva/pangakaardinumbri alusel, mis ei ole efektiivne, kui kaart on kurjategija käsutuses.

Autori arvates Eestis tegutsevad pangad üha enam rakendavad paremaid pettuste turvameetmeid, kuid siiski leidub ka nõrki kohti süsteemis, mida on võimalik kuritarvitada. Seega autori arvates ei ole süsteem veel täiesti turvaline. Samas iga tõkestamismeetmega kaasnevad ohud ning kurjategijad leiavad erinevaid viise pettuse toimepanemiseks. Seega pettust ei ole võimalik täielikult kõrvaldada, kuid autori arvates on võimalik seda tunduvalt vähendada ning leida viise, et märgata kiiremini toimepandud pettust ning reageerida vastavalt, et minimeerida võimalikku kahju.

Uurides millised on kaardipettuste tüüpilisemad näited Eestis, X3 ning X4 arvates on tüüpilisemad näited kaardi kopeerimine (*skimming*) pangaautomaadis ning X4 lisab, et ka kaardi võltsimine (X3, X4 2016, vt lisa 4 ja 5). X1 hinnangul aga Eestis on kasvamas e-kaubanduspettused (X1 2016, vt lisa 2). Alapeatüksi 2.1 on näha, et Eestis on peamiseks pettuse liigiks pettused pangaautomaatides ning järgmisena on e-kaubanduspettused.

Uurides, millised on kaardipettuste peamised põhjused peale kurjategijate kavaluse ning kaardiomanike lohakuse, X4 hinnangul peamiseks põhjuseks on ebaseadusliku tulu teenimine (X4 2016, vt lisa 5). X1 aga vastas, et pettused on peamiselt seotud süsteemi keerukusega (X1 2016, vt lisa 2). X3 arvamus kattus vastajate X1 ning X4 arvamusega, nimelt (X3 2016, vt lisa 4):

„Seni kuni on võimalus teenida ebaseadusliku tulu ja ära kasutada süsteemide nõrkusi, siis leidub alati rida isikuid, kes pettusi toime panevad.

Kui pankade süsteem või mehhanismide puudulikus lubab neid ära kasutada maksepettustes, siis eelkõige kahjustub panga maine. Edukas kaardipettus on alati

suunatud korduvale tegevusele ja seni kui pank ise midagi ette ei võta, saadakse teda ära kasutada.

Kõik toodete ja teenuste riskid tuleb ära kaardistada ja määrata riskide vähendamise sammud ning need täide viia (n: ATM antiskimmerite paigaldamine).

Klientide vaates on pangal oluline säilitada klientide usaldus. Kui kliendid tajuvad, et nende kontol olevad vahendid ei ole turvaliselt tagatud, siis kaotab pank kliendibaasi.“ (X3 2016, vt lisa 4)

Võib mõista, et väga oluline on hea maine tagamine, mida saavutatakse pakutavate toodete ja teenuste turvalisusega. Seda on märgitud ka teoreetilises osas, et pankade edu sõltub peamiselt usaldusest ja mainest.

Kui pettus aga on toime pandud ning on langetud ohvriks, peaks vastajate X1, X3 ja X4 arvamuse kohaselt esimesena panka teavitama (X1, X3, X4 2016, vt lisa 2, 4, 5). X3 lisab, et tuleb teavitada Politsei- ja Piirivalveametit (X3 2016, vt lisa 4). Et mitte langeda pettuse ohvriks, vastajate X1, X2 ja X3 hinnangul on oluline olla kliendil tähelepanelik ning ei tohi jagada isiklike andmeid (X1, X2, X3 2016, vt lisa 2, 3, 4). X4 soovituse kohaselt (X4 2016, vt lisa 5):

„*Inimestel soovitan kaardimaksete turvalisuse tagamiseks üle vaadata oma pangakaardi kasutuslimiidid, nagu sularaha väljavõtmise ja ostutehingute päevalimiidid. Limiidid aitavad vähendada võimalikust kaardipettusest tulenevat kahju, sest kaardiga ei saa teha suuri tehinguid või tühjendada kontot.“ (X4 2016, vt lisa 5)*

Et välja selgitada kas kaardipettuste eripäral Eestis on seos pankade poolt kasutusele võetud tõkestamismeetmetega, esitas autor küsitletutele viimase küsimuse 12 (vt lisa 1). X3 arvas järgmist (X3 2016, vt lisa 4):

„Pettused pannakse toime enamasti nendes riikides, kus vastavad tooted ja teenused seda võimaldavad. Seega sõltub sellest millised tooteid ja teenuseid pangad pakuvad ja kuidas on korraldatud siseriiklikud mehhanismid pettuste tõkestamises.“ (X3 2016, vt lisa 4)

X4 vastusest selgus, et pettuse tõkestamisel on väga oluline mitmete osapoolte koostöö. Vastaja arvates, miks Eesti eristub teistest riikidest, sest Eestis on kasutusel EMV

standardi kohased pangakaardid, pangaautomaatide turvalisust on suurendatud lisades täiendavaid seadmeid. Lisaks Eestis on laialdasemalt kasutusele võetud 3D turvasüsteem ning vastaja arvamuse kohaselt e-kaubandupettuste vähesuse põhjuseks on eestlaste tagasihoidlikus e-poodlemises. (X4 2016, vt lisa 5)

X1 arvamus kattub vastaja X4 arvamusega, nimelt Eestis on tugev riigisisene koostöö ning tõkestamismeetmeid rakendatakse üha laialdasemalt. Näiteks pettuste tõkestamiseks pangad on nüüdseks paigaldanud erinevaid turvaseadmeid pangaautomaatidesse ja kaardimakseterminalidesse. E-kaubanduspettuste madal arv on vastaja hinnangul seotud sellega, et Eestis on e-ostlemine veel vähe levinud. (X1 2016, vt lisa 2)

Seega võib mõista küsitletute vastustest, et kaardipettuste eripäral Eestis on seos tõkestamismeetmetega. Pangad on rakendanud mitmeid meetmeid, kaitsmaks end ning oma kliente. Näiteks mitmed riigid on alles üleminekul kiibitehnoloogiale ning peamiselt kasutatakse magnetriba tehingute teostamiseks. Eestis aga kasutatakse kiibitehnoloogiat tehingute sooritamiseks ning väga harva kohtab magnetriba kasutamist. Lisaks pangad on suurendanud tehingutekanalite turvalisust, paigaldades turvaseadmeid pangaautomaatidesse ning kaardimakseterminalidesse. E-kaubandustehingutes on aga Eesti laialdaselt kasutusele võetud 3D turvasüsteemi, mis mujal riikides ei ole niivõrd levinud. Samuti Eestis tehakse tihedat riigisisest koostööd, mis on vajalik pettuste vältimiseks. Seega rakendatud tõkestamismeetmed on üheks põhjuseks, miks Eestis on kaardipettuste osatähtsus kaarditehingute arvust väike, kuid kaarditehingute arv suur.

Praegustel pangakaartidel on peal nii kiip kui ka magnetriba. Autor soovitaks luua eraldi kiipkaardid ning magnetribaga kaardid. Magnetriba kaarti kasutatakse juhtudel kui viibitakse välismaal, kuna mitmetes välisriikides alles toimub üleminek kiibitehnoloogiale. Seega Eestis oleks kasutusel vaid kiipkaardid ning autori arvates see vähendaks oluliselt müügikohas toimuvate pettuste ohtu.

Erinevatel maksevahenditel on omad võlud ning puudused ning tehnoloogia arenguga paratamatult kaasnevad ohud. Seega autori arvates tuleb olla kurjategijatest samm eespool ning uute süsteemide loomisel arvestada süsteemi nõrkustega ning ka kõige äärmuslike võimalustega, mida võidakse kasutada kuritegevuse toimepanekuks. Lisaks autori arvates on väga suur roll kaardiomanikel, kes võivad ära hoida pettusi.

Krediidiasutused võivad luua turvalisi süsteeme, kuid kui klient seab end ohtu, ei kaitse, ükskõik kui turvaline süsteem on, see pettuse eest. Loomulikult on suur roll ka pankadel, kelle ülesandeks on tagada klientidele maksimaalne turvalisus ning võita klientide usaldus. Samuti peaksid pangad olema väga tähelepanelikud kuritegevuse suhtes ning harima kliente võimalike ohtude eest.

Erinevate Eestis tegutsevate pankade koduleheküIgedel on kirjas meelespea klientidele, kuidas vältida kaardipettuse ohvriks sattumist. Autor aga soovitab pankadel selgitada klientidele võimalikke maksepettuste skeeme, sest see võimaldab kliendil tuvastada ohuolukord ning käituda vastavalt, et mitte langeda ohvriks.

Autori arvates Eestis ei ole maksepettuste oht suur. Peamisteks põhjusteks arvab autor olevat süsteemi turvalisus ning kurjategijatele pole Eesti atraktiivne koht pettuste toime panemiseks. Samuti autori arvates eestlased on tagasihoidlikud ning ollakse tähelepanelikud maksevahendi kasutamise ajal.

KOKKUVÕTE

Maksepettused on tänapäeva ühiskonnas kasvavaks probleemiks ning pangad töötavad selle nimel, et tagada endale ning oma klientidele maksimaalne turvalisus. Maksepettuse korral kasu saamise eesmärgil kasutatakse ebaseaduslikult maksevahendit või sellelt saadavat informatsiooni. Bakalaureusetöös on vaatluse all kolmanda osapoole pettused, mille korral maksepettuse paneb toime isik, kes pole maksevahendi omanik. Sularahata maksevahendid, mida kurjategijad üritavad enim ära kasutada, on maksekaardid, tšekid ning pangaülekanded. Bakalaureusetöös on peamine rõhk maksekaardipettustel.

Uurimaks maksepettuseid ning nende tõkestamise kohta Eestis, on esitatud erialakirjanduse ülevaade ning erinevate autorite seisukohad maksepettustele. Samuti on esitatud teemakohane statistika ning vastavad küsimused spetsialistidele, et teada saada maksepettuste probleemi suuruse ning tõkestamismeetmete kohta Eestis.

Maksepettused võivad avaldada negatiivset mõju nii pangale kui ka panga klientidele, suurendades kulutusi tarbijatele, vähendades tarbijate usaldust panga poolt pakutavate toodete ja teenuste vastu ning kahjustades panga mainet.

Erialakirjanduse põhjal selgus, et maksekaardiga seotud pettuseid on võimalik jagada kaheks, nimelt pettused müügikohas ning e-kaubanduspettused. Pettused müügikohas hõlmavad kaardi magnetriba dubleerimist läbi seadme, mis on peidetud pangaautomaati või kaardimakseterminali. Peamiselt pannakse pettused pangaautomaatides ja kaardimakseterminalides toime võltsitud või varastatud/kaotatud kaartidega. E-kaubanduspettused hõlmavad aga andmete volitamata kasutamist toodete ja teenuste soetamiseks mitte näost-näkku keskkonnas. Peamiseks müügikohas toimuvate pettuste tõkestamiseks on välja töötatud kiipkaardid, millelt kurjategijatel ei ole võimalik andmeid kopeerida. E-kaubanduspettuste tõkestamismeetmeks on 3D turvasüsteem, mille korral klient autendib end läbi täiendava parooli. Samuti tehakse tehinguid ka turvaelementide CVV/CVC2 alusel, mis ei aita pettust vältida, kui kaart on kurjategija käsutuses.

Ülekandepettuse korral aga ohvrilt varastatakse isiklikud andmed ning kasutatakse, et algatada volitamata ülekanne. Petturitel on mitmeid meetmeid, et saada isiklike andmeid pettuse toimepanemiseks, näiteks *phishing*, *vishing*, *smishing* ning e-posti ohtuseadmine. Peamiselt ülekandepettuste tõkestamiseks pangad analüüsivad klientide maksetegevust ning võrdlevad klientidelt saadud andmeid pangakonto avamise ajal esitatud andmetega. Tšekipettus hõlmab aga kolme liiki, nimelt, võltsitud tšekid, muudetud tšekid ning võltsitud allkirjad. Peamiselt pangad kasutavad tšekipettuste tõkestamiseks kliendi tugevat identifitseerimist, allkirja kontrollimist ning tšeki põhjalikku uurimist, et avastada võimalikud võltsingud.

Turvalisuse saavutamine nõuab pidevat tähelepanu ning riigisisest koostööd, et saavutada väärtuslikke tulemusi. Seega erialakirjanduse põhjal võib mõista, et pankadel on võimalik rakendada mitmeid erinevaid meetmeid, tõkestamaks maksepettuseid.

Tšekipettuste ning ülekandepettuste kohta Eestis pole konkreetne statistika kättesaadav, kuna informatsioon on konfidentsiaalne. Seega autor lähtus Eesti Karistusseadustikus maksepettustele vastavatest paragrahvidest ning esitas Eestis registreeritud juhtumite arvu aastatel 2013-2015. Eesti karistusseadustikus vastavad viis paragrahvi maksepettustele, nimelt § 199. Vargus; § 213. Arvutikelmus; § 333. Maksevahendi ja väärtpaberi võltsimine; § 334. Võltsitud maksevahendi ja väärtpaberi kasutamine; § 340. Raha, pangakaardi ja muu maksevahendi, väärtpaberi, maksumärgi, postimaksevahendi ja selle jäljendi ning proovijärelevalve märgistuse võltsimise ettevalmistamine. Eestis maksepettustega seotud kuritegude eest on karistuseks vangistus või rahaline karistus. Registreeritud maksepettustega seotud juhtumite arvu põhjal võis mõista, et ülekandepettused ja tšekipettused ei kujuta suurt probleemi Eestis, kuid informatsiooni konfidentsiaalsuse tõttu ei ole võimalik konkreetset eripära võrreldes teiste Euroopa Liidu riikidega esitada.

Eestis toimunud kaardipettuste statistika aga on kättesaadav ning selgus, et Eestis, võrreldes naaberriikidega, on kõrge kaarditehingute arv kuid väike kaardipettuste arv. Samuti Eestis on võrreldes teiste Euroopa Liidu riikidega madal kaardipettuse osatähtsus kaarditehingute arvust. Lisaks kaardipettuste statistikast selgus, et Eesti oli 2013. aastal peamiseks pettuse tehingukanaliks pangaautomaat, kuid teistes Euroopa Liidu riikides oli

peamiseks pettuse tehingukanaliks e-kaubandus. Võib mõista, et Eestis, võrreldes teiste Euroopa Liidu riikidega, ei kujuta kaardipettused suurt ohtu.

Uurimaks Eestis tegutsevate pankade poolt kasutusele võetud maksepettuste tõkestamismeetmete kohta, koostas autor küsimustiku, millele vastas neli spetsialisti. Küsitletute vastustest selgus, et Eestis tegutsevad pangad kontrollivad tšekil esitatud allkirja ning identifitseerivad kliente, vältimaks tšekipettuseid. Ülekandepettuste vältimiseks aga pangad jälgivad kliendi maksetegevust ning Eestis on määratud tehingulimiit, mida on võimalik teostada paroolikaardiga. Kaardipettuste tõkestamiseks on Eesti pangad laialdaselt kasutusele võtnud 3D turvasüsteemi, mis ei ole teistes riikides niivõrd levinud. Aktiivselt on kasutusel ka kiipkaardid, mis on oluliselt vähendanud kaardipettuseid müügikohas. Lisaks selgus küsitletute vastustest, et Eestis tehakse tugevat riigisisest koostööd kaardipettuste tõkestamiseks ning pangad on paigaldanud lisaseadmeid pangaautomaatidesse ja kaardimakseterminalidesse, et vältida pettuse ohtu. Bakalaureusetöö teoreetilises osas samuti selgus, et kliendi identifitseerimine, allkirja kontrollimine ning kliendi maksetegevuse jälgimine on peamised tõkestamismeetmed, vältimaks tšekipettuste ning ülekandepettuste ohvriks sattumist. Samuti kaardipettuste võimalikud pangapoolsed tõkestamismeetmed on kiibitehnoloogia ning 3D turvasüsteem, mille kasutatavus mitmetes riikides on veel väike.

Võib öelda, et Eestis on pangad laialdaselt kasutusele võtnud erinevad maksepettuste tõkestamismeetmed ning see on üheks põhjuseks, miks Eestis on maksepettuste arv madal. Autori arvates Eestis ei ole maksepettuste oht suur, mille peamisteks põhjusteks on süsteemi turvalisus ning eestlaste tähelepanelikkus maksevahendi kasutamise ajal.

Autor soovitab tšekipettuste vähendamiseks pankadel harida kliente, selgitades, millised on pettuslikud tšekid. Ülekandepettuste vähendamiseks aga harida kliente pettuste skeemide kohta, kuidas kurjategijad koguvad andmeid. Teadmine skeemidest võimaldab klientidel ära tunda ohuolukorra ning käituda vastavalt, et mitte langeda pettuse ohvriks. Samuti pankadel loobuda paroolikaartide väljastamisest ning nõuda tehingute teostamist ID kaardi alusel.

Maksekaardipettuste vähendamiseks soovitab autor pankadel väljastada eraldi kiipkaardid ning magnetribaga kaardid, et Eestis oleksid kasutusel vaid kiipkaardid.

Magnetriba kaardid oleksid kasutusel vaid viibides välismaal, kuna mitmed riigid on alles üleminekul kiibitehnoloogiale, seega tehinguid on võimalik teostada vaid magnetriba alusel.

Maksepettused on seotud mitmete osapooltega, näiteks maksepettuste tõkestamine hõlmab ka kaupmehi. Bakalaureusetöös on keskendutud vaid pangapoolsetele tõkestamismeetmetele, seega on võimalik uurida ka teiste maksesüsteemiga seotud osapoolte püüdlusi maksepettuste tõkestamiseks. Samuti on võimalik uurida, kuidas on korraldatud siseriiklikud mehhanismid pettuste tõkestamiseks ning osapoolte vahel koostöö tõhustamiseks, et tagada maksimaalne turvalisus. Kuna maksepettuste teema on väga lai, on võimalik bakalaureusetööd edasi arendada magistritööks.

VIIDATUD ALLIKAD

1. **Ahven, A., Leps, A., Tammiste, B., Salla, J., Tamm, K., Kraas, K., Tüllinen, K., Kaldur K. K., Kruusmaa, K-C., Lindsalu P., Rohtla, R., Solodov, S., Kõiv, T.** Kuritegevus Eestis 2015. Justiitsministeerium, 2016, 132 lk. [http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/kuritegevus_eestis_2015.pdf]. 19.05.2016
2. Australian payments fraud details and data. Australian Payments Clearing Association 2015, 23p. [http://www.apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2015.pdf]. 10.03.2016
3. Card-Not-Present Fraud: A Primer on Trends and Authentication Processes. Smart Card Alliance, 2014, 21p. [http://www.smartcardalliance.org/resources/pdf/CNP-WP-012414.pdf]. 26.01.2016
4. Card payments in Europe – a renewed focus on SEPA for cards. European Central Bank, 2014, 78p. [https://www.ecb.europa.eu/pub/pdf/other/cardpaymineu_renfoconsepaforcards201404en.pdf]. 24.04.2016
5. Card present fraud. CreditCards.com, 2016. [http://www.creditcards.com/glossary/term-cardpresent-fraud.php]. 26.01.2016
6. Check Fraud Prevention. JPMorgan Chase. [https://www.jpmorgan.com/tss/General/Check_Fraud_Prevention/11147353909 15]. 26.01.2016
7. Cheques&Cheque Clearing The Facts. A guide to cheques and the UK cheque clearing system. Cheque and Credit Clearing Company, 2012, 65p [http://www.chequeandcredit.co.uk/files/candc/press/cheques_the_facts_2012.pdf]. 27.01.2016

8. **Chiezey, U., Onu A. J. C.** Impact of Fraud and Fraudulent Practices on the Performance of Banks in Nigeria. British Journal of Arts and Social Sciences, Vol. 15, No I, 2013, p12-28, 17p. [http://www.bjournal.co.uk/paper/BJASS_15_1/BJASS_15_01_02.pdf]. 02.01.2016
9. **Christiansen, P.** Four important trends shaping the future of credit cards. First Data Corporation, 2011, 10p. [http://cloud1.firstdata.com/downloads/thought-leadership/cc-trends-wp.pdf]. 23.04.2016
10. **Conroy, J.** Card-Not-Present Fraud in a Post-EMV Environment: Combating the Fraud Spike. RSA, 2014, 14p [https://community.rsa.com/servlet/JiveServlet/downloadBody/40320-102-1-11023/card-not-present-fraud-post-emv-env-wp.pdf]. 20.02.2016
11. Credit card fraud**:** How to fight it**...** (cover story). Credit Management, 2009, p26-27, 2p. URL: http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=100&sid=854f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bth&AN=39363407
12. **Dhameja, S., Jacobs, K., Porter, R. D.** Clarifying liability for twenty-first-century payment fraud. Economic Perspectives, 2013, Vol. 37, No. 3, p107-129, 23p. [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2386037]. 26.01.2016
13. Dissecting Wire Fraud: How it Happens, and How to Prevent It. Guardian Analytics, 2013, 11p. [www.aba.com/Tools/Offers/Documents/Dissecting_Wire_Fraud_WP_Dec2013.pdf]. 30.01.2016
14. **Engler, T. C**. Payments fraud. Smart Business Pittsburgh, 2015, Vol. 22 Issue 3, p28-28. 1p. URL: http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=95&sid=854

f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bth&AN=108649535

15. Fighting wire fraud: An industry perspective. ACI Worldwide, 2013, Vol 1, 7p. [http://www.aciworldwide.com/-/media/files/collateral/fighting-wire-fraud-v1-tl-us-5143-0613.pdf]. 30.01.2016
16. Fourth report on card fraud. European Central Bank, 2015, 27p. [https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf]. 25.03.2016
17. Fraud. Oxford Dictionaries. [http://www.oxforddictionaries.com/definition/english/fraud]. 02.01.2016
18. Fraud prevention and data protection, A Eurofinas-ACCIS Report on Fighting Fraud in Consumer Lending. Eurofinas and ACCIS, 2011, [http://www.eurofinas.org/uploads/documents/Non-visible/Eurofinas-Accis_ReportOnFraud_WEB.pdf]. 26.01.2016
19. Fraud the facts 2015. Financial Fraud Action UK, 2015, 60p [http://www.financialfraudaction.org.uk/Fraud-the-Facts-2015.asp]. 26.01.2016
20. Fraud Remains a Risk with EMV Chip Cards. Teller Vision, 2016, Issue 1461, p8-8, 3/4p.
    URL:
    http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=9&sid=854f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=117&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=111811555&db=bth
21. **Froud, D**. The Central role of authentication in fighting fraud in mobile commerce. Journal of Payments Strategy&Systems, 2015/2016, Vol 9, Issue 4, p274-279, 6p.
    URL:
    http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=90&sid=854f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bth&AN=113145957

22. **Gates, T., Jacob, K.** Payment Fraud: Perception Versus Reality- A conference summary. Economic Perspectives, 2009 1st Quarter, Vol. 33 Issue 1, p7-15, 9p. URL: http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=85&sid=854f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bth&AN=37019172
23. Karistusseadustik. Vastu võetud Riigikogus 6. juunil 2001. aastal. –Riigi Teataja I osa, 2001, nr. 61, art. 364. [https://www.riigiteataja.ee/akt/184411]. 10.05.2016
24. **King, D.** Chip-and-PIN:Success and Challenges in Reducing Fraud. Retail Payments Risk Forum, 2012, 25p. [http://www.cse.unsw.edu.au/~meyden/3441/chip_and_pin.pdf]
25. **Matheswaran, P., Siva Sankari, E., Rajesh, R.** Fraud Detection in Credit Card Using DataMining Techniques. International Journal for Research in Science Engineering and Technology, 2015, Vol 2, Issue 1, p 11-18, 8p. [http://ijrset.in/20152102.pdf]. 26.01.2016
26. Mittefinantsettevõtete ja kodumajapidamiste sularahata makstavate maksete arv makseviisi lõikes (tükki). Eesti pank, 2016. [http://statistika.eestipank.ee/?lng=et#listMenu/2211/treeMenu/FINANTSSEKTOR/620/965]. 25.03.2016
27. Mittefinantsettevõtete ja kodumajapidamiste sularahata makstavate maksete käive makseviisi lõikes (miljon eurot). Eesti pank, 2016. [http://statistika.eestipank.ee/?lng=et#listMenu/2210/treeMenu/FINANTSSEKTOR/620/965]. 25.03.2016
28. **Patidar, R., Sharma, L.** Credit Card Fraud Detection Using Neural Network. Iinternational Journal of Soft Computing and Engineering, 2011, Volume-1, Issue-NCAI2011, p32-38, 7p [http://ijsce.org/attachments/File/NCAI2011/IJSCE_NCAI2011_025.pdf]. 26.01.2016
29. Payment and securities settlement systems in the European Union: non-euro area countries. Volume 2. European Central Bank, 2007, 411p.

[https://www.ecb.europa.eu/pub/pdf/other/ecbbluebooknea200708en.pdf?f32dcde157ce03bab03d869e3a65a559]. 10.05.2016

30. Payment cards. Interpol. [http://www.interpol.int/Crime-areas/Financial-crime/Payment-cards]. 26.01.2016
31. Payment Fraud. Europol. [https://www.europol.europa.eu/ec3/payment-fraud]. 26.01.2016
32. Payment Fraud Law & Legal Definitions. USLegal. [http://definitions.uslegal.com/p/payment-fraud/]. 26.01.2016
33. Payment Statistics for 2014. Press release. European Central Bank, 2015, 7p. [https://www.ecb.europa.eu/press/pdf/pis/pis2014.en.pdf?d9feb0268bb38b960b806ea69b6bf467]. 20.05.2016
34. Report on card fraud. European Central Bank, 2012, 17p. [https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201207en.pdf?1c24d5c720e014b7c67c7df665701775]. 25.03.2016
35. **Ruankaew, T**. Beyond the Fraud Diamond. International Journal of Business Management & Economic Research, 2016, vol. 7, issue 1, p. 474-476, 3p. URL: http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=80&sid=854f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bth&AN=113035733
36. **Sakharova, I.** Payment card fraud: Challenges and solutions. IEEE International Conference on Intelligence & Security Informatics, 2012, p227-234, 8p DOI: 10.1109/ISI.2012.6284315
37. Second report on card fraud. European Central Bank, 2013, 22p. [https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf]. 25.03.2016
38. Single Euro Payments Area (SEPA). European Commission, 2016. [http://ec.europa.eu/finance/payments/sepa/index_en.htm]. 25.03.2016
39. Stop Check Fraud Before It Starts. Teller Vision, 2001, issue 1285, p1, 2p.

URL:
http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=70&sid=854f0279-f107-4fa3-8b40-b9cb485fc67d%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=6763383&db=bth

40. **Sullivan, R. J.** The Changing Nature of U.S. Card Payment Fraud: Indrustry and Public Policy Options. Economic Reviw, 2010 2nd Quarter, Vol. 95 Issue 2, p101-133, 33p
URL:
http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=7&sid=1211ef79-7992-4038-844c-9e1970074de1%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=a9h&AN=51789275

Controlling Security Risk and Fraud in Payment Systems. Economic Review, 2014 3rd Quarter, p5-36. 32p
URL:
http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=4&sid=1211ef79-7992-4038-844c-9e1970074de1%40sessionmgr103&hid=127&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bth&AN=98764805

41. **Summers, B. J.** Fraud containment. Economic Perspectives, 2009, 1 Quarter, vol. 33, issue 1, p17-21, 5p.
URL:
http://eds.a.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=2&sid=070f2956-4a75-42f3-bac9-b74dd5768e70%40sessionmgr4004&hid=4213&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=37019173&db=bth

42. The Payment System. European. Central Bank, 2010, 369p [https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf]. 26.01.2016

43. Third report on card fraud. European Central Bank, 2014, 22p.

[https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf]. 25.03.2016

44. **Turner, P. S., Wunnicke D. B.** Check fraud: beware standard bank agreements! Journal of Corporate Accounting & Finance (Wiley), 2004, Vol. 16 Issue 1, p45-48, 4p.
DOI: 10.1002/jcaf.20071
45. What you need to know about check fraud. Fifth Third Commercial Banking. 10p
[https://www.53.com/doc/cm/cm-check-fraud-guide.pdf]. 26.01.2016
46. Wire Fraud Prevention. Fiserv, 2014.
[http://www.financialcrimerisk.fiserv.com/WorkArea/DownloadAsset.aspx?id=8518]. 30.01.2016
47. **Wolfe, D. T., Hermanson, D. R**. The Fraud Diamond: Considering the Four Elements of Fraud. CPA Journal, 2004, vol. 74, issue 12, p. 38-42, 4p.
URL:
http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=2&sid=2b12abee-693f-4fcd-ac46-cf6a5afc7e90%40sessionmgr103&hid=117&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=15290416&db=bth
48. **Woodfield, M.** Check fraud: Is your business protected? Las Vegas Business Press, 2013 Supplement, p18-18. 1/4p.
URL:
http://eds.b.ebscohost.com.ezproxy.utlib.ut.ee/eds/detail/detail?vid=4&sid=2b12abee-693f-4fcd-ac46-cf6a5afc7e90%40sessionmgr103&hid=117&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=90373439&db=bwh
49. **X1.** Kaardipettuste tõkestamise spetsialist. Autori intervjuu. Helisalvestis. Tallinn, 23. märts 2016.
50. **X2.** Maksetoimkond, kaartide töögrupp. Autori küsitlus. Elektronposti kiri. Tallinn, 24. märts 2016.
51. **X3.** Rahapesu tõkestamise toimkond, järelvalveametnik. Autori küsitlus. Elektronposti kiri. Tallinn, 30. märts 2016.

52. **X4.** Makse- ja arveldussüsteemide osakonna spetsialist. Autori küsitlus. Elektronposti kiri. Tallinn, 10. mai 2016.

LISAD

Lisa 1. Spetsialistidele esitatud küsimused

1. Miks Eestis ei ole tšekkide maksevahend levinud?
2. Millised on Eestis kasutusel olevad meetmed, et vältida tšekipettuseid?
3. Kuidas hindate ülekandepettuseid Eestis ning millised on tüüpilisemad näited?
4. Millised on peamised ülekandepettuste tõkestamismeetmed?
5. Kuidas hindate maksekaardipettuste levikut Eestis? Kas see on viimase viie aasta jooksul pigem suurenenud või vähenenud?
6. Millised on peamised kasutusel olevad kaardipettuste tõkestamismeetmed?
7. Kas kasutusel olevad tõkestamismeetmed on piisavad pettuste tõkestamiseks?
8. Millised on maksekaardipettuste tüüpilisemad näited Eestis?
9. Millised on maksekaardipettuste peamised põhjused (peale kurjategijate kavaluse ning kaardiomanike lohakuse)?
10. Millised on peamised soovitused, et mitte langeda kaardipettuste ohvriks?
11. Kuhu tuleks pöörduda kui on langetud pettuse ohvriks?
12. Euroopa Keskpanga poolt 2015. aastal avaldatud aruandest on näha, et Eesti eristus 2013. aastal teistest riikidest järgmiste tegurite poolest:

- Eestis on suur tehingute arv, kuid väike pettuste arv pangakaardi kohta.
- Eesti oli 2013. aastal ainuke Euroopa Liidu riik, kus peamiseks pettuse tehingukanaliks oli pangaautomaat. Eesti naaberriikides olid e-kaubandustehingud suurima pettuse osatähtsusega.
- Eestis on pettuse osatähtsus kaarditehingute arvust väga väike (0,02%) ning asub väikseima pettuse osatähtsusega riikide seas.
- Miks Eesti eristub teistest riikidest loetletud tegurite poolest ning kas sellel on seos kasutuselolevate tõkestamismeetmetega?

Lisa 2. Vastajaga X1 tehtud intervjuu vastused

Kuidas hindate kaardipettuste levikut Eestis viimase viie aasta jooksul?

See on nagu subjektiivsete parameetritega. Kui võtame kaardipettused, soovitan sul Keskpanga raportit vaadata. Kõik kategooriad, väga objektiivsed hinnangud läbi aastate. Aga üleüldiselt Eesti ja Baltimaad on madalama riskiga piirkond. Et aga see ongi see, et miks see on niimodi. Sest tegelikult kui kaarti kasutada, siis riske on vähe, et neid kopeeritakse või kuritarvitatakse. Et mida rohkem kaarte kasutatakse, seda rohkem pettuseid on, et tuleb vaadata proportsioone, palju tegelikult inimesed kasutavad, kuidas nad seda kasutavad. Kui vaadata summasid, siis kindlasti, et mis on keskmine summa, sest ongi see, et näiteks Prantsusmaa, seal kasutatakse kaarte hästi palju, raha inimestel on olemas, summad suured, kui pettus toimub siis ka pettus suurem, pettusi palju. Eesti on raporti kontekstis väga madala riskiga maa. Kusjuures Eestis huvitav see, et eriline piirkond, kus kaardimaksed on kõige levinumad, makstakse palju, aga *fraudi* või pettuste risk väike. Joonistelt aga näha, et mida rohkem kasutatakse, seda rohkem on näha ka pettuseid. Ja näiteks kui Leedu, kus kaardimaksed pole levinud nagu Eestis, seal näha et proportsioonid on täpselt paigas, makseid vähe ja pettust vähe. Eestis makstakse palju aga pettusi vähe.

Millised on peamised kaardipettuste tõkestamismeetmed Eestis?

Üleminek manetribalt kiibile mis toimus umbes 1995 aastal. See oli kõige suurem samm. Me läksime vanast tehnoloogiast uuele. Magnetribal staatilised andmed on kasutatud, mis ei ole krüpteeritud, neid saab lihtsalt uuesti kasutada ja kopeerida. Kiibi puhul on see, et seal on mikroprotsessor, iseenesest seda kopeerida ei saa, see lihtsalt töötab niimodi. Ehitatud niiviisi, et selle töösse ei ole võimalik sekkuda. Kuna tegemist on rahvusvahelise standardiga, siis seda jälgitakse ja koguaeg uuendatakse.

See magnetriba mis praegu kaardi peal on, kümnete aastatega muutunud ei ole. Aga vaadates kiipi mis seal on, seda on uuendatud kolm korda päris tõsiselt. Visuaalselt pole seda näha, aga just krüptograafilised operatsioonid mis siin käivad. Siiamaani käib arutelu, kas seda on kuidagigi võimalik ära kasutada, et on olemas mingid tööd selle kohta. Ja ikkagi kui vaadata võimalused välja toodi, tekib teine küsimus, et kas on

otstarbekas üldse rünnak läbi viia, sest see pole kindlasti nii efektiivne kuritegevus kui magnetriba. Magnetribal ostad 30 euroga seadme, kopeerid ära ja sul on dublikaat olemas.

Kui me räägime *aga card not present* tehingutest, siis tegelikult kõik algas sellest, et iseenesest kaart oli alguses mõeldud kasutusele *card present enviromentis*. Kliendil tekkis hiljem vajadus, kus oli helistamise peale tehingud jne. Algul oli *card number* ja aegumiskuupäev. Siis tuli välja turvaelement CVC2 või CVV2. See on krüpteeritud väärtus, mida tuleb sisestada. Selle väärtuse kohta on eraldi protseduurid, kuidas kaupmehed peavad seda käitlema. Kogu kaarditehingute kohta käib väga väga palju igasuguseid regulatsioone, kuidas kaardimakse tegelikult peab toimuma. Esialgu oli see CV2 kood, mis noh see kunagi oli samm edasi, aga praegu vaadates pole midagi, ainuke kaitse on see, et see on teisel pool kaarti. Järgmine samm oli 3D *secure* protokoll ning kaardiomanik autendib end täiendava parooliga. See on protokolli moodi rohkem. Sest kui me räägime mitte 3D *secure* tehingutest, maksete tegemine käib nii, et kaupmees saab kaardi, põhimõtteliselt kõik andmed edastatakse kaardi väljastajale, kes kontrollib kas kõik andmed olemas ja klapib, kas raha on olemas. Kui kõik andmed on olemas, vastab kaupmehele, et korras, võib kaupa väljastada. Kui tegemist on 3D *secure* protokolliga, siis makse on keerulisem. Kaupmees saab kaardi, mis on 3D *secure* toega, enne tehingu teostamist ta suunab seda väljastajale või väljastaja esindajale. *Issure* küsib ja oskab kuvada arvutis või telefonis täiendavat autentimist, mis ei ole üldse kaupmehega seotud. Kaupmees seda ei näe ja pole süsteemis. See ongi see väljastaja ja kliendi vahel. Klient autnendib ennast kas staatilise parooliga, täiendava parooliga. Siis kui ta kinnitab ennast, siis *issuer* saadab kaupmehele, et klient on olemas, on identifitseeritud ja tehingut saab sooritada. See on tunduvalt nagu keerulisem skeem. See on nagu maksete tehnoloogia, mis mingisugused riskid vähendab. Sest näiteks kui kaupmees saab andmed kätte siis tekivad sealt riskid, näiteks CVV2, andmed võivad olla hea eesmärk ründajale. Sest kui tegemist on suure kaupmehega, seal andmeid palju.

Kas need meetmed on piisavad?

See ei lahenda probleemi, kuidas *issuer* identifitseerib klienti. Kui *issuer* identifitseerib klienti staatiliste parooliga ehk staatiliste andmetega, siis kerkivad teised riskid, näiteks kolmas osapool, kes kontrollib arvutit ja liiklust seal, on teoorias võimalik neid

kompromiteerida. Hetkel süsteem pole täiuslik, nõrgad kohad sees, näiteks magnetriba, mida igapäevaselt kasutatakse väga harva, kuid eksisteerib pangakaardil.

Kas arendatakse välja ka uusi tõkestamismeetmeid?

Pigem praegu milles probleemid on, siis näiteks kiibitehingud, kui vaadata ringi Eestis, siis keegi eriti ei mõtle magnetribast ja ma arvan, et suht imelikult vaadatakse, et mille jaoks seda vaja on. Kui vaadata EMVco leheküljele, see on see kiibi standardi pidaja, siis minu meelest viimased maailmaandmed olid need, et kolmandik maksetest oli kiibimaksed. *Back to reality*. Euroopa ja Eesti on kiibimaa, aga näiteks Ameerika eelmine aasta alles hakkas liikuma. Vaadates mahtusi, Eesti väga suurt rolli ei mängi ja kogu aeg mõeldakse uusi tõkestamismeetmeid välja.

Millised on tõkestamismeetmete negatiivsed küljed?

Negatiivne on see, et tegelikult magnetriba tehnoloogia on. Miks seda kasutatakse, see on väga lihtne ja kaart on odav. Ei ole palju osapooli. Kui pettusi ei ole, siis tegelikult kui vaadata ärimudelit, siis on tehniliselt väga kerge impleminteerida, kaupmehe kulud väiksed, protsessori kulud väiksed.

Millised on tüüpilisemad kaardipettuste näited Eestis?

Praegu kõige kiiresti kasvav trend on interneti pettused. Lihtne seletada, sest internetis tehingute arv kasvab. Samas suht palju kasutatakse ka kaardinumbri ja CV2 alusel tehinguid. Kui me räägime kiibist, siis kiip on rohkem levinud kui 3D *secure* süsteem. Alati saab leida kohta, kus kuritarvitada siukseid lihtsaid andmeid. Aga see ongi see kaardi võlu ja probleem. Üheltpoolt on see taskus maksevahend, mida saad kasutada terves maailmas. Kui kasutad siis ei mõelda, et midagi juhtub, tuletad meelde PIN koodi ja ülejäänud töö teevad sinu eest mitu panka ja süsteemi. See on väga standardiseeritud valdkond, et tagada kindlust. Aga tegemist on väga läbipaistva kanaliga. Kliendi poolt on tähtis, et väga paindlik maksevahend, samas kui on väga palju süsteeme ja kuidas aktsepteerida, siis on lahti ebaturvalised viisid, näiteks magnetriba. Kui vaadata palju kaarti kasutatakse ja võrreldes pettustega, siis pettusi vähe.

Millised on kaardipettuste peamised põhjused?

Siin osapooli on palju ja süsteem väga keeruline. Põhimõtteliselt kuna kaarti kasutatakse rahvusvaheliselt, et klient ostab Amazonis, ise asudes Berliinis, tema pank on Eestis, et selles mõttes süsteem on keerukas ning kohti, kus keegi saab eksida või keegi saab kuritarvitada on palju. Näiteks kui vaadata statistika, kõige suuremad põhjused ongi infolekked. Kuna Magnetriba on vana tehnoloogia, see on tunduvalt atraktiivsem kurjategijatele, sest informatsiooni hea kuritarvitada.

Kuhu peab pöörduma pettuse korral ja millised on soovitused klientidele, et mitte langeda ohvriks?

No klient võiks olla tähelepanelikum ja ei tohi jagada andmeid kellelegi. Kui aga tegemist on pettusega, ehk kui tuvastad midagi, mida ei peaks olema, siis esimese asjana panka teavitama. Sealt edasi protsessid, kuidas sind aidata. Aga no pigem ongi see, et esimene kontakt pank.

Miks Eestis ei ole tšekkide makseviis levinud ja millised on peamised tõkestamismeetmed?

Sellepärast ei kasuta tšekke, see ei ole mugav. Pettus on maksevahenduse tagajärg. Ameerikas tšekid olid väga populaarsed, Eestis tšekke üldse ei ole kunagi olnud populaarsed, ei anna võrreldagi. Küll pank võtab vastu tšekke, aga protsess range. Väga range, sest petuse risk suur, peamiselt allkirja kontrollimine ja kliendi identifitseerimine ja uuritakse, et näha pettust. Oli juhtum, kus klienti peteti tšekkidega, kus lihtsameelsed võtsid tšekid vastu, läksid panka ja pank ütles, et see katmata tšekk. Selline makseinstrument on iseenesest väga riskantne.

Kuidas hindate ülekandepettuseid Eestis, millised on tõkestamismeetmed?

See ei ole nii levinud Eestis. Sest ikkagi kui vaadata, kus me näeme probleemi või survet kurjategijate poolt, on see sama paroolikaart, kus põhimõtteliselt, no viimasel ajal pole näinud sessiooni ülevõtmist. Pigem labane *vishing*, kust kliendilt küsitakse andmeid ja klient lahkelt jagab neid paroolikaardilt. Selliseid on olnud ja tundub, et klient on ikka siiamaani kõige nõrem lüli. Aga samas Eestis on pandud maksimaalne summa limiidiks,

et kui teostada paroolikaardiga makse, suuremad summad aga ID kaardiga. Et seega see pole nii atraktiivne kurjategijatele.

Internetipank on lihtsam kui kaart, sest tegemist on ühe süsteemiga ja ühe keskkonnaga. Internetipank on kinnisem süsteem kui kaardid. Internetipangas on ka teatud riskid olemas, sessiooni ülevõtmine jne.

Euroopa Keskpanga poolt 2015. aastal avaldatud aruandest on näha, et Eesti eristus 2013. aastal teistest riikidest järgmiste tegurite poolest:

- **Eestis on suur tehingute arv, kuid väike pettuste arv kaardi kohta.**
- **Eesti oli 2013. aastal ainuke Euroopa Liidu riik, kus peamiseks pettuse tehingukanaliks on pangaautomaat. Eesti naaberriikides olid e-kaubandustehingud suurima pettuse osatähtsusega.**
- **Eestis oli pettuse osatähtsus kaarditehingute arvust väga väike (0,02%) ning asub väikseima pettuse osatähtsusega riikide seas.**
- **Miks Eesti eristub teistest riikidest loetletud tegurite poolest ning kas sellel on seos kasutuselolevate tõkestamismeetmetega?**

Minuarust on Eestis väga tugev koostöö riigi sees ning see kindlasti pettute arvu vähendab. Just erinevad kanalid, pangad, kaupmehed on tugevas koostöös ja aina laialdasemalt on tõkestamismeetmed kasutusel. Pangad on nüüdseks pannud turvaseadmeid pangaautomaatidele ja kaardimakseterminalidesse, kuna skimmingu rünnakute arv hakkas kasvama. Internetipettuste korral 3D *secure* süsteemi kasutamine on suur. Madal *card not present* pettuste arv on pigem seotud veel sellega, et Eestis internetis väga ei maksta kaupade eest.

Lisa 3. Vastaja X2 küsimuste vastused

Pangakaartide valdkonnas (kus mina toimetan) on kiipkaardile üleminekuga toimunud oluline hüpe turvalisuse kasvus, sisuliselt ei ole kiipi võimalik murda. Samuti toimub pidev kiibi põlvkondade uuendamine ja kaasajastamine. Euroopa on juba ammu kiibile üle läinud, kuid Ameerikas on alanud ning Aasias käimas juba mõnda aega. Kuna nendes regioonides on prevaleeriv magnetriba kasutamine, siis näeme jätkuvalt just sealtpoolt rohkem väärkasutamist. Selles olukorras keskenduvad petturite ründed rohkem just magnetriba tehnoloogiale, mis on kopeeritav ning taaskasutav. Selle vastu võitlemiseks on hulk meetodeid, mille hulgas lisakontrollid ning parmeetrid kliendile (nt kui ei ole välismaal siis muude riikida kasutamine kinni keerata, sama näiteks e-kommertsi osas). Samuti on kaardil endal turvaelemendid sh magnetribal ning muidugi on pankadel tehingute turvamonitooring, mis on väga oluline meetod väärkasutuse vältimiseks. Sellise väärkasutuse vältimiseks on oluline ka kliendil olla teadlik ja mitte luua ülearuseid riskiolukordasid, soovitan lugeda http://www.seb.ee/foorum/igapaevased-rahaasjad/kuidas-kasutada-pangakaarti-turvaliselt

Teine suund mida püütakse ära kasutada on e-kommerts, kuid juba aastaid on kasutusel 3DSecure tehnoloogia, mis põhineb kliendi tugeval autentimisel (vt internetist lähemalt vajadusel).

Tehnoloogia arenguga tekib alati uusi ahvatlusi ning proovijaid, maailmas on levimas kontaktivabad kaardimaksed ning kaugel ei ole aeg kui kaardid kolivad mobiili. Kindlasti püütakse ka neid lahendusi murda, kuid meie ülesanne on olla ees.

Mis puudutab numbreid ja mahtusid, siis neid ma otseselt jagada ei saa aga kindlasti leiad laiemaid turu ülevaateid ka netist. Võrreldes kunagise magnetriba ajaga on toimunud pettuste oluline vähenemine ja viimaste aegade mahutrendis ei ole hüppeid.

Lisa 4. Vastaja X3 küsimuste vastused

Miks ei ole Eestis tšekkide maksevahend levinud?

Tšekkidest loobumine on minu hinnangul seotud otstarbekusega. Kui on olemas finantssüsteem, mis katab ära tšekkidega seotud vajadused, siis need heidetakse kõrvale. Pankadele on tšekkidega seonduv liiga suur kuluartikkel ning kui välist surved antud teenusele ei ole, siis pole asjakohane pidada üleval tervet osakonda.

Millised on Eestis kasutusel olevad meetmed, et vältida tšekipettuseid?

AS SEB Pank ei tee tehinguid tšekkidega, mistõttu antud segmendiga seonduvates pettustes meid ära kasutada ei saa.

Kuidas hindate ülekandepettuseid Eestis ning millised on tüüpilisemad näited?

Eesti krediidiasutustes liiguvad vahendid kontode vahel väga kiiresti, siis on oht olla ärakasutatud just PayPal laadsete toodetega. Isiku esitatud tellimustes muudetakse sissemurdmise teel andmeid ja kliendi vahendid laekuvad võõrale kontole krediidiasutuses, kus need kas kantakse kohe edasi või võetakse ATM kaudu välja mõnes teises riigis.

Internetipangaga seotud pettused on minu hinnangul enamasti seotud sellega, et kliendi arvutisse on sisse murtud ja varastatud andmeid, mis võimaldavad edukalt pettust korda saata. Pankadele on oluline info kiire saabumine pettusest. Enamasti märkavad kannatanud pettust liiga hilja ja vahendeid ei ole võimalik koheselt või piiratud mahus tagasi saada.

Peamiselt internetipank on seotud paroolide vargustega. Tooksin välja andmete vargust, mis võimaldab petturil vahendeid hõlpsasti kliendi nimel mujale kanda.

Millised on peamised ülekandepettuste tõkestamismeetmed?

Riske vähendavateks meetmeteks on monitoorida laekumisi ja seada kliendi kontodele märkeid koheste laekumiste piiramiseks. Muu hulgas on ohumärgiks kui klient soovib avada või on juba avanud mitmeid kontosid, millel puudub selge põhjendus. Oluline on kiire info saamine pettuse toimepanemise kohta.

Kuidas hindate maksekaardipettuste levikut Eestis? Kas see on viimase viie aasta jooksul pigem suurenenud või vähenenud?

Kaardipettuste arv on viimastel aastatel olnud isikliku hinnangu kohaselt tõusutrendis. Turule on tulnud rida instrumente, mis on loonud soodsa pinnase kõikvõimalike maksepettuste läbiviimiseks.

Millised on peamised kasutusel olevad kaardipettuste tõkestamismeetmed?

Üheks meetmeteks on monitoorida laekumisi. Monitooringu käigus võib selguda, et antud isikute tehingud ei ole läbipaistvad ja isik võib panna toime pettuse.

Puuduseks on teadmatus. Pank ei suuda alati enda monitooringu tulemusena võimalikku pettust ära hoida.

Pankadel on väga oluline, et oleksid selged tegevuskavad olemas enne pettuse toimepanemist, selle teadasaamisel ning ka hiljem. Tähtis on monitoorida ja kaardistada isikuid, kes võivad olla seotud tulevaste pettustega. Juhul kui pank saab teada pettusest, siis kontole olevad vahendid blokeeritakse kahtluse asjaolude uurimiseks.

Kas kasutusel olevad tõkestamismeetmed on piisavad pettuste tõkestamiseks?

Kasutusel olevad meetmed on tõhusad üksnes piiratud ulatuses ja need peavad jätkuvalt astuma turul olevate finantstoodetega ühte sammu.

Kui ka meetmed oleks väga tõhusad, siis ei oleks see absoluutne. Edukas pettuse tõkestamine on enamasti seotud kiire reageerimisega petta saanud isiku poolt. Kui krediidiasutusele infot pettuse kohta ei laeku, siis ei pruugi kahjuks ka pank pettuse toimepanemisest teada. Seega ei ole tõhusust võimalik alati mõõta pankade poolt kehtestatud meetmetega

Millised on maksekaardipettuste tüüpilisemad näited Eestis?

Kaardipettused on enamasti seotud skimmeritega ATMis. Ka sel juhul on tegemist andmete vargusega, mis võimaldab petturil vahendeid pangaautomaadi kaudu välja võtta.

Millised on maksekaardipettuste peamised põhjused (peale kurjategijate kavaluse ning kaardiomanike lohakuse)?

Seni kuni on võimalus teenida ebaseadusliku tulu ja ära kasutada süsteemide nõrkusi, siis leidub alati rida isikuid, kes pettusi toime panevad.

Kui pankade süsteem või mehhanismide puudulikus lubab neid ära kasutada maksepettustes, siis eelkõige kahjustub panga maine. Edukas kaardipettus on alati suunatud korduvale tegevusele ja seni kui pank ise midagi ette ei võta, saadakse teda ära kasutada.

Kõik toodete ja teenuste riskid tuleb ära kaardistada ja määrata riskide vähendamise sammud ning need täide viia (n: ATM antiskimmerite paigaldamine).

Klientide vaates on pangal oluline säilitada klientide usaldus. Kui kliendid tajuvad, et nende kontol olevad vahendid ei ole turvaliselt tagatud, siis kaotab pank kliendibaasi.

Millised on peamised soovitused, et mitte langeda kaardipettuste ohvriks?

Mitte anda enda mis tahes koode ja paroole teistele isikutele. Pettust aitab vältida heas mõttes kriitilisus ja tähelepanelikkus.

Kuhu tuleks pöörduda kui on langetud pettuse ohvriks?

Pettuse, kelmuse ning muudel analoogsetel juhtumitel tuleb koheselt teavitada enda krediidiasutust ja Politsei- ja Piirivalveametit. Krediidiasutustel on võimekus koheselt pettuse teatele reageerides teha vastavaid toiminguid, mis võivad peatada vahendite väljumist krediidiasutusest. Politseid on vaja teavitada kriminaalmenetluse alustamiseks.

Euroopa Keskpanga poolt 2015. aastal avaldatud aruandest on näha, et Eesti eristus 2013. aastal teistest riikidest järgmiste tegurite poolest:

- **Eestis on suur tehingute arv, kuid väike pettuste arv kaardi kohta.**
- **Eesti oli 2013. aastal ainuke Euroopa Liidu riik, kus peamiseks pettuse tehingukanaliks oli pangaautomaat. Eesti naaberriikides olid e-kaubandustehingud suurima pettuse osatähtsusega.**

- **Eestis on pettuse osatähtsus kaarditehingute arvust väga väike (0,02%) ning asub väikseima pettuse osatähtsusega riikide seas.**
- **Miks Eesti eristub teistest riikidest loetletud tegurite poolest ning kas sellel on seos kasutuselolevate tõkestamismeetmetega?**

Pettused pannakse toime enamasti nendes riikides, kus vastavad tooted ja teenused seda võimaldavad. Seega sõltub sellest millised tooteid ja teenuseid pangad pakuvad ja kuidas on korraldatud siseriiklikud mehhanismid pettuste tõkestamises

Lisa 5. Vastaja X4 küsimuste vastused

Miks ei ole Eestis tšekkide maksevahend levinud?

Ma usun, et peamine põhjus on selles, et pangandusvaldkonnas tegi kaardimakse areng suuri edusamme just ajal, mil tšekkide periood ei olnud veel jõudnudki oluliseks kasvada. Teisisõnu, Eestis jäi tšekkide kui makseviisi kasutus arenguetapina lihtsalt vahele. Teistpidi võiks öelda, et elektrooniliste kanalite areng oli piisavalt kiire ja nö peberil toimivad, aeglased ja tülikad tšekid ei tundunud atraktiivsed. Põhimõtteliselt võib öelda, et oli see turu loomulik ja väga positiivne areng, kuid ilmselgelt aitasid sellele kaasa ikka pangad krediitkaartide pakkumisega! Lõuna Euroopas, nt Prantsusmaal seevastu on tšekkidega arveldamist veel väga palju ja neil ei õnnestu omal ajal juurdunud harjumusest kuidagi lahti saada.

Millised on Eestis kasutusel olevad meetmed, et vältida tšekipettuseid?

-

Kuidas hindate ülekandepettuseid Eestis ning millised on tüüpilisemad näited?

-

Millised on peamised ülekandepettuste tõkestamismeetmed?

-

Kuidas hindate maksekaardipettuste levikut Eestis? Kas see on viimase viie aasta jooksul pigem suurenenud või vähenenud?

Eestis on kaardipettuste arv teiste riikidega võrreldes väike. Üldjuhul on kaardipettusi vähem neis riikides, kus kasutatakse ka vähe kaardimakseid, näiteks Bulgaarias ja Horvaatias. Eesti ja Soome aga paistavad silma nii aktiivse kaardikasutuse kui ka väheste kaardipettuste poolest. Eesti eristub teistest Euroopa riikidest internetipettuste vähesuse poolest.

Millised on peamised kasutusel olevad kaardipettuste tõkestamismeetmed?

Kaardipettus on enamasti rahvusvaheliselt organiseeritud tegevus, mille tõkestamine eeldab üleeuroopalist koostööd ning ennetavate meetmete ja rahvusvaheliste standardite kasutuselevõtmist. Kaardipettuste tõkestamiseks on keskpangad, pangad ja kaardiskeemid teinud juba märkimisväärseid jõupingutusi ning võtnud kasutusele lisameetmeid, et muuta kaardimaksed turvalisemaks. Ühtses euromaksete piirkonnas vahetatakse magnetribad sujuvalt välja turvalisema kiibitehnoloogia vastu, mis vähendab kaardipettusi ja kaartide kopeerimist.

Kuna kaardiga makstavate e-ostude ja muude interneti vahendusel tehtavate ostude arv aina suureneb, on vaja pöörata üha rohkem tähelepanu e-ostude turvalisuse tagamisele. Euroopa Liidu keskpangad ja järelevalveasutused makseteenuse pakkujatele välja töötanud miinimumnõuded, et tagada internetis tehtavate maksete turvalisus. Interneti vahendusel tehtavate maksete puhul aitab pettuste vähenemisele kaasa 3D turvasüsteemi kasutamine: internetis kaardiga maksmisel tuleb sisestada täiendav kood, mis sisuliselt täidab PIN-koodi ülesannet. Seda süsteemi on Eestis tegutsevad pangad aktiivselt juurutamas (Verified by Visa, MasterCard SecureCode).

Sularahaautomaatide ja kaardimakseterminalide pettusi saab vähendada siis, kui üha rohkem riike, sh väljaspool SEPA ala, võtavad kasutusele pangakaartide võltsimist takistava rahvusvahelise standardi kaardimakse autoriseerimiseks (EMV standardi), kus info salvestatakse magnetriba asemel kiibile ja kaardiomanik tuvastab end PIN-koodiga.

Kas kasutusel olevad tõkestamismeetmed on piisavad pettuste tõkestamiseks?

Pangad ja kaardiorganisatsioonid töötavad pidevalt selle nimel, et muuta oma kaardid ning makselahendused veelgi turvalisemaks. Aga ka kaardi valdaja ise saab palju ära teha. Kuna pangakaardi limiidid aitavad vähendada võimalikust kaardipettusest tulenevat kahju, võiks inimesed üle kontrollida, kas pangakaardi kasutuslimiidid, nagu sularaha väljavõtmise ja ostutehingute päevalimiit, vastavad endiselt vajadustele ega ole ebamõistlikult kõrged. Eesti pangad suurendavad pidevalt pangaautomaatide turvalisust, lisades pangakaardi võltsimise ja kopeerimise vastaseid seadmeid (nn anti-skimmer'eid), kuid täielikku kaitset ei taga ükski turvalahendus ega anti-skimmer.

Kuna kurjategijate eesmärk on kätte saada kaardi PIN-kood, võib pangaautomaadi juurde olla paigaldatud videokaamera või lisaklaviatuur, mistõttu tasub enne pangaautomaadis toimingu tegemist jälgida kaardi sisestusava ja klaviatuuri ning nende ümbrust. PIN-koodi sisestades on mõistlik klaviatuuri ka varjata.

Millised on maksekaardipettuste tüüpilisemad näited?

Kaardiandmete pettusliku kättesaamise viisidest üks tüüpilisemaid on kaardi kopeerimine (skimming), lisaks veel kaardi võltsimine (counterfeit). Pangaautomaatides kaardi kopeerimisel on pangaautomaadi kaardiava külge kurjategijate poolt paigaldanud vastav seade ehk skimmer, mis kopeerib kaardi magnetribalt andmed ja need saadetakse edasi (tavaliselt kas USAsse või mõnda Aasia riiki), kus kaardi peale uuesti andmed kirjutatakse, ja seejärel võetaksegi raha välja.

Millised on maksekaardipettuste peamised põhjused (peale kurjategijate kavaluse ning kaardiomanike lohakuse)?

Ilmselt on kaardipettuse toimepanemise peamine põhjus kuritegelikul teel ebaseadusliku kasu saamine.

Millised on peamised soovitused, et mitte langeda kaardipettuste ohvriks?

Inimestel soovitan kaardimaksete turvalisuse tagamiseks üle vaadata oma pangakaardi kasutuslimiidid, nagu sularaha väljavõtmise ja ostutehingute päevalimiidid. Limiidid aitavad vähendada võimalikust kaardipettusest tulenevat kahju, sest kaardiga ei saa teha suuri tehinguid või tühjendada kontot.

Kaardi igapäevasel kasutamisel tasub meeles pidada järgmist:

- Poes makstes või sularahaautomaati kasutades jälgida, et PIN-kood ei oleks sisestamisel teistele nähtav.
- PIN-koodi ei tohi kirjutada kaardile või hoida seda muul viisil salvestatuna kaardiga koos.

- Ärge valige PIN-koodi, mis on kergesti äraarvatav (näiteks teie sünniaasta või lihtsad numbrikombinatsioonid 1234, 1122, 1111 jne).

- PIN-kood on kaardi elektrooniline allkiri. PIN-koodiga kinnitatud kaardimakset kaardi valdaja vaidlustada ei saa.

- Kaardimakse tuleb teha kaardi valdaja juuresolekul. Teenindaja ei tohi minna kaardiga tagaruumi.

- Tasub olla tähelepanelik, kui sularahaautomaadi välimus on tavatu: kaardi sisestuse koha juures on ebaharilikke osi, kaarti on raske sisestada või kätte saada jne. Nimelt on esinenud juhtumeid, kus varas paigaldab automaadile kaardi kopeerimise seadme, millega tuvastatakse kaardi magnetriba andmed. Varastatud kaardiandmetega proovitakse võtta välja sularaha või teha oste välisriikides, kus magnetribapõhised tehingud on veel võimalikud.

Kuhu tuleks pöörduda kui on langetud pettuse ohvriks?

Kaardipettuse ohver peab kohe ühendust võtma oma pangaga. Kui inimene ise ei ole pettuse toimumises süüdi, saab ta varastatud raha mõne aja jooksul tagasi. Ka kaardi kadumisel tuleks teavitada oma panka ja paluda kaart blokeerida.

Euroopa Keskpanga poolt 2015. aastal avaldatud aruandest on näha, et Eesti eristus 2013. aastal teistest riikidest järgmiste tegurite poolest:

- **Eestis on suur tehingute arv, kuid väike pettuste arv pangakaardi kohta.**
- **Eesti oli 2013. aastal ainuke Euroopa Liidu riik, kus peamiseks pettuse tehingukanaliks oli pangaautomaat. Eesti naaberriikides olid e-kaubandustehingud suurima pettuse osatähtsusega**
- **Eestis on pettuse osatähtsus kaarditehingute arvust väga väike (0,02%) ning asub väikseima pettuse osatähtsusega riikide seas.**
- **Miks Eesti eristub teistest riikidest loetletud tegurite poolest ning kas sellel on seos kasutuselolevate tõkestamismeetmetega?**

- Pettuste tõkestamise osas SEPA alal üldiselt ütleksin seda, et pettuse vähendamisele aitavad kaasa mitmed osapooled – keskpangad ja järelevalveasutused on välja töötanud internetimaksete turvalisuse nõuded. Need nõuded puudutavad esiteks üldiseid riskide juhtimise soovitusi, teiseks väga konkreetseid turvanõudeid internetimaksetele, näiteks on oluliselt rangemad ka kliendi autentimise osas (staatilise PIN koodi asemel nõutakse mittestaatilist turvakoodi). Keskpangad ja järelevalveasutused on nõuded välja töötanud, kuid reaalselt hakkavad neid rakendama st nende nõuete rakendamisega turvalisust tõstma makseteenusepakkujad, st pangad, kaardiskeemid, kaupmehed. Ja keskpankade järelevaatajad ning järelevalveasutused on alustanud nõuete täitmise kontrollimist. Seega, kaardipettustega võitlevad mitmed osapooled, igal-ühel on selles oma roll.

  Eesti paistab tõepoolsest silma kaardipettuse madala taseme poolest. Eestis on kaardipettuste tõkestamiseks tehtud järgnevat:

- Eestis antakse välja vaid EMV standardi kohaseid ehk kiibiga varustatud turvalisemaid pangakaarte;

- võitlemaks kurjategijate poolt automaatidele paigaldatavate skimmerite vastu on Eestis tegutsevad pangad paigaldanud oma pangaautomaatidele täiendavaid turvaseadmeid.

- teiste Euroopa riikidega võrreldes on Eestis internetipettusi neli korda vähem, kuna siin on rangemad turvanõuded ulatuslikumalt kasutusele võetud – e-kaubanduse pettuse tõkestamiseks on Eestis tegutsevad pangad väga laialdaselt kasutusele võtnud 3-D Secure komponendi (pangakaardid on liidetud 3D-Secure süsteemiga). 3D Secure süsteem võetakse kasutusele selleks, et ostude sooritamine maksekaardiga oleks veelgi turvalisem kui enne. Põhimõtteliselt on 3D turvasüsteemi puhul tegemist täiendava makse täiendava autentimisega. Internetipoes ostu sooritamisel tuleb tavapäraselt märkida oma kaardi number, tähtaeg ja turvakood, siis 3D turvasüsteemi kasutamise puhul küsitakse täiendavat autoriseerimist, milleks reeglina on Internetipanga kasutajatunnuse ja autoriseerimiskoodi sisestamine. Selline täiendav autoriseerimine takistab

pettuseid internetipoodides, kuid samuti suurendab oluliselt maksekaardi kasutamise turvalisust ja kaitset. Selle puhul on oluline, et mitte ainult pangakaardid ei oleks liidetud turvasüsteemiga, vaid et ka kaupmehed st e-poed kasutavad sellist tuvastamisprotseduuri ja muudaksid oma süsteemid turvaliseks. Seega, jälle on vajalik erinevate osapoolt koostöö turvalisuse saavutamisel!

Kahtlemata võib lisaks sellele, et Eesti pangad on kasutusele võtnud turvaliste kaardimaksete protseduuri 3D Secure , internetipettuste vähesuse üks põhjuseid olla ka eestlaste suurem tagasihoidlikkus e-ostlemisel.

SUMMARY

PAYMENT FRAUD AND ITS PREVENTION IN ESTONIA

Britta Kiviking

Payment fraud is a growing problem in today's society and banks need to protect themselves and their clients form possible frauds. For this, banks are required to develop a variety of payment fraud prevention measures. In payment fraud for profit, means of payment or its information are unlawfully used. This study consist of different payment fraud types: card fraud, wire fraud and cheque fraud, while the main emhasis is on card fraud. This topic is very timely because payment fraud continues to grow. This study focuses on the measures of preventing payment frauds in banks which will help to protect the banks and their customers from potential threats.

The goal of this bachelor´s thesis is to find out the speciality of payment frauds in Estonia and the connection to its prevention strategies. It is important to find out whether payment frauds pose a major threat to Estonia and what preventive measurues are implemented to prevent fraud.

To achieve this goal, the author set the following reasearch tasks:

- define the content of payment fraud,
- present and explain different frauds connected to means of payments,
- on the basis of speciality literature present possible techniques for preventing payment frauds,
- find out the spread of payment fraud in Estonia and its uniqueness,
- find out techniques of preventing payment fraud on the basis of the author's inquery,

- compare the results of the inquery and data in theoretical part and present suggestions for lowering payment fraud.

The most used means of payment in Estonia are payment cards. Payment card fraud can be categorized into two major groups: card not present fraud and card present fraud. To prevent card present fraud, a chip technology is widely used and in card not present fraud a 3D secure system is used. This study showed that Estonia is different from European Union Member States in many ways. Namely, Estonia has high number of card transactions but small number of card fraud. Also in 2013 the main fraud channel was ATM, but in single euro payments area the maine fraud channel was card not present.

To combat payment fraud actions, Estonia uses strong internal co-operation and apply strong preventive actions to ensure maximum security. For example, Estonia uses chip card technology and 3D secure system which is not very common in other countries. These methods have been proven to reduce the number of card frauds significantly.

Due to the confidentiality of information, statistics for cheque fraud and wire fraud are not available. Thus, it is not possible to bring out any reliable information about these types of frauds. Nevertheless, wire payments are a mayor payment form in Estonia and it is crucial to take measures against this type of fraudulant activity. For this, banks monitor customer's banking operations and limit password-dependent transation amounts. For cheque frauds banks also check signatures and identify customers.

To conclude the author's opinion, Estonian banks have obtained many techniques for preventing payment frauds and it may be one of the main reasons why the number of payment frauds is low in Estonia. Due to the security of Estonian banks and the attention to means of payments of estonian people, the danger of payment frauds is low in Estonia. Author suggest that in order to reduce to level of card fraud, banks should issue magnetic stripe cards for payments in other countries and chip cards separately for transactions made in home. As for wire frauds, banks should discard the use of password-dependent transactions and use ID card-dependent transactions only. Also, for cheque fraud banks should display fake cheque examples on their websites and in their offices to increase awearness of fraudulent cheques. To sum up, in order to be more effective in securing

financial transactions, banks should pay more attention to educating and rising awearnes of people on the dangers of payment frauds.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Britta Kiviking,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
   Maksepettused ja nende tõkestamine Eestis,
   mille juhendaja on dotsent Nadežda Ivanova,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **24.05.2016**