Hantering av CNP-kortbedrägerier

Ett arbete om hur banker kan förhindra och förebygga kortbedrägerier

Max-Erik Björkqvist

Examensarbete
Företagsekonomi
2021

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Företagsekonomi
Identifikationsnummer:	23567
Författare:	Max-Erik Björkqvist
Arbetets namn:	Hantering av CNP-kortbedrägerier Ett arbete om hur banker kan förhindra och förebygga kort-bedrägerier
Handledare (Arcada):	Patrik Pehrsson
Uppdragsgivare:	

Sammandrag:
Detta examensarbete behandlar motarbetet av CNP-kortbedrägerier, som i dagens läge anses vara väldigt vanliga i samhället. Arbetets syfte är att presentera vad banker kan göra för att bekämpa bedrägliga CNP-korttransaktioner samt försök till dessa. Bekämpningen av bedrägliga korttransaktioner kan delas upp i två kategorier, det arbetet som görs för att hitta samt hindra dessa, och det arbetet som görs för att förebygga dessa. De två huvudkategorierna bildar tillsammans en klar helhetsbild om ämnet som studeras. Arbetets teoridel presenterar olika typer av produkter, processer och teorier som läsaren behöver för att förstå helhetsbilden. I teoridelen presenteras även bakgrundsinformation om bedrägerier, internetbrott och CNP-kortbedrägerier. Teoridelen av arbetet berör kort även teman som phishing, dataintrång, och Tor-nätet, det vill säga källorna varifrån de kriminella kan få tag på dessa kortuppgifter. Till sist presenteras processer och verktyg som banker kan använda för att förhindra kortbedrägerier. Datainsamlingsmetoden som används i detta arbete är kvalitativa intervjuer. För att få pålitlig information om ämnet utfördes det sammanlagt tre semistrukturerade intervjuer med respondenter som under en längre period har arbetat på finansbranschen och kan anses vara specialister inom ämnet. Urvalsmetoden som använts i arbetet är ändamålsenligt urval. Data som fåtts i intervjuerna representerar endast respondenternas personliga åsikter och den tar ingen hänsyn till något företags eller andra tredjeparters upplevelser eller åsikter om ämnet. Datat har analyserats och ur den har det identifierats processer och faktorer som bidrar till det förhindrande, samt förebyggande arbetet av CNP-kortbedrägerier. Resultaten förstärker de processer och metoder som framkommit i teoridelen av arbetet. Transaktionsmonitorering, maskininlärning och väl utförda CPP-analyser lyfts fram som viktiga faktorer inom bekämpande av CNP-kortbedrägerier. Resultaten kan anses reliabla vid denna, samt närliggande tidpunkt men kommer antagligen att påverkas av nya verktyg och processer som i fortsättningen integreras i verksamheten.

Nyckelord:	Kortbedrägeri, CNP, Bedrägeri, Internetbrott, Identitetsstöld, Bekämpningsmetod, Bank
Sidantal:	52
Språk:	Svenska
Datum för godkännande:	

DEGREE THESIS	
Arcada	
Degree Programme:	Business administration
Identification number:	23567
Author:	Max-Erik Björkqvist
Title:	Hantering av CNP-kortbedrägerier Ett arbete om hur banker kan förhindra och förebygga kortbedrägerier
Supervisor (Arcada):	Patrik Pehrsson
Commissioned by:	

Abstract:

This thesis has its focus on CNP fraud management. Card fraud is considered very common in today's society. The purpose of this thesis is to present what banks can do to fight fraudulent CNP card transactions and transaction attempts. The fight against fraudulent card transactions can be divided into two categories, the work that is done to find and stop them, and the work that is done to prevent them. The two categories together form a clear overall picture of the subject that is being studied. The theoretical framework of the thesis presents different types of products, processes, and theories that the reader needs to understand to get the overall picture. The theoretical framework also presents background information on fraud, cybercrime and CNP card fraud. The theoretical framework also touches on topics such as phishing, data breaches, and the Tor network, i.e., the sources from where the criminals can obtain the card information they need. Lastly, in the theoretical framework, fraud management tools and processes that banks can use to fight CNP card fraud are presented. The data collection method used in this work is qualitative interviews. To obtain reliable information on the subject, three semi-structured interviews were conducted with respondents. The respondents have worked in the financial industry for a long period and can be considered specialists in the subject. The method used to select respondents in the thesis is purposive choice of participants. The data obtained in the interviews only represents the respondents' personal opinions and does not consider any companies or other third party's experiences or opinions on the subject. The data has been analyzed and after that, processes and factors that contribute to the two main categories of CNP card fraud has been identified. The results confirm the processes and methods that have emerged in the theoretical framework of the thesis. Transaction monitoring, machine learning and well-executed CPP analyzes are highlighted as important factors in fraud management. The results can be considered reliable at this point of time, as well as the near future, but will probably be affected by new tools and processes that will be integrated into the business in the future.

Keywords:	Kortbedrägeri, CNP, Bedrägeri, Internetbrott, Identitetsstöld, Bekämpningsmetod, Bank
Number of pages:	52
Language:	Swedish
Date of acceptance:	

OPINNÄYTE	
Arcada	
Koulutusohjelma:	Liiketalous
Tunnistenumero:	23567
Tekijä:	Max-Erik Björkqvist
Työn nimi:	Hantering av CNP-kortbedrägerier Ett arbete om hur banker kan förhindra och förebygga kortbedrägerier
Työn ohjaaja (Arcada):	Patrik Pehrsson
Toimeksiantaja:	

Tiivistelmä:
Tämä opinnäytetyö käsittelee CNP-korttipetosten estävää ja ennaltaehkäisevää työtä. Korttipetoksia pidetään nyky-yhteiskunnassa hyvin yleisinä. Opinnäytetyön tarkoituksena on esitellä, mitä pankit voivat tehdä torjuakseen maksukorttipetoksia ja niiden yrityksiä. Maksukorttipetosten torjuntatyö voidaan jakaa kahteen kategoriaan, niiden löytämiseen ja estämiseen sekä ennaltaehkäisevään työhön. Nämä kaksi kategoriaa muodostavat yhdessä selkeän kokonaiskuvan tutkittavasta aiheesta. Työn teoreettisessa osassa esitellään erilaisia tuotteita, prosesseja ja teorioita, joita lukija tarvitsee kokonaiskuvan ymmärtämiseksi. Teoriaosio tarjoaa myös taustatietoa petoksista, internet-rikoksista ja CNP-korttipetoksista. Työn teoreettisessa osassa käsitellään lyhyesti myös teemoja, kuten kalastelua, tietomurtoja ja Tor-verkkoa eli lähteitä, joista rikolliset voivat saada käsiinsä korttitietoja. Lopuksi esitellään prosesseja ja työkaluja, joita pankit voivat käyttää korttipetosten torjunnassa. Tässä työssä on käytetty kvalitatiivisia haastatteluja tiedonkeruumenetelmänä. Luotettavan tiedon saamiseksi tehtiin yhteensä kolme semistrukturoitua haastattelua. Vastaajat ovat työskennelleet rahoitusalalla pitkään ja heitä voidaan pitää aiheen asiantuntijoina. Vastaajien valinnassa on käytetty valintatapana tarkoituksellista valintaa. Haastatteluissa saadut tiedot edustavat vain vastaajien henkilökohtaisia mielipiteitä, eikä niissä ole otettu huomioon minkään yrityksen tai muiden kolmansien osapuolten kokemuksia tai mielipiteitä aiheesta. Aineisto on analysoitu ja niistä on tunnistettu prosesseja ja tekijöitä, jotka parantavat CNP-korttipetosten estävää sekä ennaltaehkäisevää työtä. Tulokset vahvistavat työn teoreettisessa osassa esiin tulleita prosesseja ja menetelmiä. Transaktiomonitorointi, koneoppiminen ja hyvin suoritetut CPP-analyysit nousevat esille tärkeinä tekijöinä CNP-korttipetosten torjunnassa. Tuloksia voidaan pitää luotettavina tässä hetkessä sekä lähitulevaisuudessa, mutta luotettavuuteen tulee vaikuttamaan uudet työkalut ja prosessit, joita tulevaisuudessa integroidaan liiketoimintaan.

Avainsanat:	Kortbedrägeri, CNP, Bedrägeri, Internetbrott, Identitetsstöld, Bekämpningsmetod, Bank
Sivumäärä:	52
Kieli:	Ruotsi
Hyväksymispäivämäärä:	

INNEHÅLL

Figurer

1 INLEDNING

I och med att samhället blir alltmer digitalt, förändras människornas liv och vanor. Vem kan i dagens läge föreställa sig leva utan en mobiltelefon eller social media? Att bära kontanter ses även i dagens läge som opraktiskt och riskabelt. Vissa affärer tar numera inte ens emot kontanter. I stället bär människor i dag bank- och kreditkort. Betalkorten anses vara praktiska och säkra, och det är de också. Historien visar dock att där det finns en vilja, så finns det en väg.

Digitaliseringen av samhället har även påverkat de kriminellas metoder, kanske till och med gynnat dem. Digitaliseringen av samhället har skapat nya plattformar, där de kriminella kan utöva sina brott. Sociala media, Tor-nätet och andra liknande plattformar är bra exempel på ställen där de kriminella kan utöva sina brott. Brotten i säg har dock inte förändrats, de bara utförs på nya sätt. I dagens läge behöver de kriminella inte längre se sina offer i ögonen. I stället kan de sitta hemma, i ett café eller till och med på andra sidan av jorden. Detta innebär att de kriminella bättre kan dölja sin identitet och därefter minimera risken att åka fast. Verktygen de kriminella använder för att utföra brotten har också förändrats. I stället för att bära vapen, utnyttjar de kriminella i dagens läge datorteknik. Gårdagens ficktjuv, håller idag på med internetbrott, som till exempel kortbedrägerier (Gottschalk 2010 s. 10, Brenner 2012 s. 8–13).

Oavsett hurdant bedrägeri det är frågan om, är syftet alltid det samma, att skaffa sig ekonomisk framskridande på någon annans bekostnad. Detta gäller även för betalkortsbedrägerier. Betalkortsbedrägerier är vardag i dagens samhälle och de görs ständigt många sådana. Den svenska polismyndigheten (2019) hävdar att CNP-kortbedrägerier ökade med 134 procent mellan åren 2014 och 2019 (Polismyndigheten 2019). Kortbedrägerierna görs ofta från utlandet och löses i praktiken aldrig (Vuorimäki 2020). Det kan man förstå eftersom det enligt den svenska polismyndigheten (2019) anmäls ett bedrägligt CNP-kortköp var femte minut.

Som med andra ekonomiska brott, såsom till exempel penningtvätt, har banker en stor roll i att känna igen och förhindra CNP-kortbedrägerier. Banker arbetar hårt och utvecklar ständigt säkerheten och identifieringsmetoderna kring nätbetalningar, men samtidigt så lär sig de kriminella nya och framför allt bättre metoder för att utföra kortbedrägerier.

Sanningen är att det pågår ett sorts spel av katt och råtta, där parterna tävlar om vem som har högre kort i handen (Puurunen 2018).

I detta arbete presenteras processer och metoder som banker kan använda för att bekämpa bedrägliga CNP-betalkortstransaktioner samt försök till dessa.

1.1 Problemformulering

Betalkortsbedrägerier är ett vardagligt problem som påverkar flera parter och förorsakar kostnader åt enskilda kortinnehavare, banker, liksom företag i alla former och storlekar. Ämnet påverkar hela samhället och det är kanske just därför ämnet blir så intressant. ”I en masteruppsats som beställts av polisens nationella bedrägericenter framgår det att de samhällsekonomiska kostnaderna för bedrägeribrott, där ett bedrägligt kortköp gjorts utan det fysiska kortet, under 2018 uppgick till närmare 2 miljarder kronor” (Polismyndigheten 2019).

I inledningen av detta arbete har jag presenterat ämnet, samt motiverat dess relevans i samhället. Samtidigt har det genomförts flera undersökningar där tyngdpunkten har lagts på att förklara och undersöka kortbedrägerier som fenomen. Det finns dock inte många undersökningar med focus på motarbetandet av dessa. Om man utgår från att det Vuorimäki (2020) hävdar är sant, kan man dra den slutsatsen att banken är den sista parten i kedjan som kan förhindra ett kortbedrägeri från att ta plats. Detta väcker än fråga: använder banker all den information som finns om ämnet och är deras processer för att bekämpa CNP-kortbedrägerier tidsenliga? Därmed är det motiverat att studera, undersöka och sprida den kunskap, samt de processer och metoder banker kan använda för att förhindra samt förebygga kortbedrägerier.

1.2 Syfte och frågeställning

Detta examensarbetes syfte är att presentera vad bankerna kan göra för att bekämpa bedrägliga CNP-betalkortstransaktioner samt försök till dessa. Bekämpningen av bedrägliga korttransaktioner kan delas upp i två kategorier, arbetet som görs för att hitta samt förhindra dem, och arbetet som görs för att förebygga dem. De två huvudkategorierna

bildar tillsammans en klar helhetsbild som svarar på själva frågan: *Hur bekämpar banker bedrägliga betaltransaktioner och deras försök på kortinnehavarnas betalkort?*

Frågeställningen i detta arbete är följande:

1. Vilka metoder används för att förhindra CNP-kortbedrägerier i banken?

2. Hur kan banker förebygga CNP-kortbedrägerier?

1.3 Avgränsningar och förväntat resultat

Bedrägliga korttransaktioner påverkar inte bara kortinnehavarna, utan flera parter i samhället. Kedjan som påverkas av dessa kortbedrägerier kan till exempel bestå av parter som kortinnehavaren, banken och företagen där korttransaktionerna görs. Ämnet i sig, är mycket brett och innehåller olika slags sorter av kortbedrägerier och subkategorier till dessa.

Detta examensarbete koncentrerar inte i sig på kortbedrägerier, utan har i stället focus på deras bekämpning. Forskningen är avgränsad så att den endast tar ställning till bekämpningen av så kallade CNP-kortbedrägerier, det vill säga kortbedrägerier där kortet inte är fysiskt på plats medan kortets uppgifter används till bedrägligt syfte. Fenomen som till exempel ”skimming” studeras inte.

Specialister som arbetar med bekämpning av kortbedrägerier på banker har intervjuats för att få svar på forskningsfrågorna i examensarbetet. Resultaten är avgränsade till deras professionella synpunkt och tar inte hänsyn till något företags, polisens eller andra tredje parters upplevelser eller erfarenheter om ämnet.

Mina personliga förväntningar är att examensarbetet presenterar processer, verktyg och metoder som banker kan använda för att bekämpa bedrägliga CNP-betalkortstransaktioner samt dess försök. Arbetet kommer även framföra hur verktygen och metoderna fungerar i verkligheten.

1.4 Arbetets struktur

Arbetets teori behandlas i det andra kapitlet. Kapitlet framför olika typer av betalkort, korttransaktioner och betalningsprocesser. Kapitlet presenterar även information om internetbrott, bedrägerier och CNP-kortbedrägerier. Kapitlet berör också teman som phishing, dataintrång och Tor-nätet, det vill säga källorna varifrån de kriminella får tag på dessa kortuppgifter. Till sist presenteras processer och verktyg som banker kan använda för att förhindra kortbedrägerier. Det tredje kapitlet jämför olika metoder och presenterar den metod som har använts i detta examensarbete. Kapitlet presenterar även urvalsmetoden som använts, tillvägagångssättet och reliabiliteten. Det fjärde kapitlet presenterar resultaten av den empiriska delen av arbetet och analyserar dem. Femte kapitlet presenterar slutsatser som kan dra på basen av de fynd man gjort i det föregående kapitlet. Arbetet avslutas med diskussion i det sjätte kapitlet.

2 TEORI

Denna del i detta arbete koncentrerar sig på att ge läsaren den insikt och de verktyg hen behöver för att förstå det komplexa ämnet som studeras. Den teoretiska ramen täcker, förklarar och binder de mest relevanta och centrala begreppen och processerna i arbetet. Informationen som presenteras i denna del är samlad från relevanta källor.

2.1 Kortbetalningsindustrin

För att man skall kunna undersöka och förstå hur man förhindrar och förebygger kortbedrägerier, är det viktigt att man först och främst förstår vad kortbedrägerier är. Man måste även veta hur kortbetalningar egentligen fungerar, hur pengarna rör sig och vilka de centrala aktörerna i den långa kedjan är. Denna del av arbetet framför historien, centrala begrepp i branschen och introducerar produkter samt verktyg som används i branschen.

2.2 Betalkort

Betalkort beviljas åt konsumenter av kortutfärdaren som oftast är banker. Kortet klassificeras som antingen privatkort eller företagskort beroende på till vilket ändamål betalkortet beviljas. Personliga betalkort är de kort som beviljas av banker eller andra finansiella institutioner till privatpersoner för personligt bruk. Till personliga betalkort kan även beviljas parallellkort för till exempel familjemedlemmar. Företagskort beviljas till ett företag eller dess anställda och kan endast användas av behöriga personer. Företagskort kan inte användas för personligt bruk utan måste användas för kostnader som är arbetsrelaterade som till exempel resekostnader och representationskostnader (European Central Bank 2014 s. 15).

2.2.1 Kreditkort

Kreditkort gör det möjligt för kortinnehavaren att göra inköp både på nätet och vid en betalterminal samt ta ut kontanter från en bankautomat. Varje kreditkorts innehavare har en beviljad kreditgräns som beror på hur mycket pengar hen tjänar samt hur mycket lån och annan skuld kortinnehavaren har. Krediten kan användas till fullo och när den är slut kan kortinnehavaren inte använda kortet före hen har betalat bort hela eller en del av skulden. Kortinnehavaren får en räkning varje månad från kortutgivaren varifrån hen kan se samt granska sina inköp. På räkningen syns oftast de centrala uppgifterna om de inköp kortinnehavaren har gjort. Dessa är datum, summa, inköpsställe, valuta och ibland även kurs ifall inköpet är slutfört i en utländsk valuta. Oftast erbjuder kortutgivaren en minimisumma (som till exempel 3% av den totala använda krediten) som måste betalas in på kortutfärdarens konto senast på räkningens förfallodag. Ifall kortinnehavaren betalar bort en del av skulden, kan kortet endast användas upp till den summa kortinnehavaren har tillgängligt kredit. Ifall kortinnehavaren inte betalar bort hela skulden utan i stället betalar bort minimisumman, kan hen räkna med att få betala ränta på sin skuld. Det är alltså frågan om en så kallad betala efter köpet modell (European Central Bank 2014 s. 15, Nordea Bank Oyj. 2021).

2.2.2 Debetkort

Debetkort gör det möjligt för kortinnehavaren att göra inköp både på nätet och vid en betalterminal samt ta ut kontanter från en bankautomat. Transaktionerna som kortinnehavaranen gör debiteras från kortinnehavarens bankkonto. Debetkortets uttagningsgräns är den summa som ligger på kortinnehavaren bankkonto. Det är med andra ord alltså inte möjligt att spendera mera pengar än kunden i själva verket har (European Central Bank 2014 s. 15, Nordea Bank Oyj. 2021).

2.2.3 Kombikort

Ett kombikort är ett betalkort med både debet- och kreditsida. Eftersom kortet har två sidor (kredit och debet), har kortet även två olika kortnummer. Kortnumret som finns på framsidan av kortet står för kreditsidan, medan kortnumret som finns på kortets baksida står för debetsidan av kortet. Kortet gör det möjligt för kortinnehavaren att göra inköp både på nätet och vid en betalterminal samt ta ut kontanter från en bankautomat. Kortinnehavaren kan själv välja om hen vill använda kredit eller debetsidan för ett genomföra ett inköp. Kortkrediten på ett kombikort fungerar på samma sätt som ett kreditkort (Nordea Bank Oyj. 2021).

2.2.4 Förbetalda-kort (Prepaid kort)

Förbetalda-kort är den sällsyntaste varianten av betalkort vi ser i samhället. Förbetaldakort fungerar på samma sätt som debetkort, dvs. det är möjligt för kortinnehavaren att göra inköp både på nätet och vid en betalterminal samt ta ut kontanter från en bankautomat. Den främsta skillnaden mellan förbetalda-kort och debetkort är att kortinnehavaren måste ladda in saldo på det förbetalda kortet för att kunna köra köp senare. Kortet är alltså inte kopplat till kortinnehavarens bankkonto och uttagningsgränsen på kortet är den summa kortinnehavaren har ladda in på kortet (European Central Bank 2014 s. 15).

2.3 Betalningstransaktioner

Betalkortsindustrin använder olika kategorier för korttransaktioner som görs. I vilken kategori korttransaktionen hör beror på om kortet är närvarande vid köpet eller inte. Nästa del förklarar skillnaden på de olika korttransaktionerna och hur de kategoriseras.

2.3.1 CP-transaktioner

Ifall kortet eller kortinnehavaren är fysiskt närvarande när transaktionen görs kategoriseras transaktionen som card-present (CP). CP-korttransaktionen sker då kortet fysiskt är på plats och placeras in i en maskin som till exempel betalningsterminal eller bankautomat. Maskinen läser informationen på kortet från antingen magnetbandet på baksidan av kortet eller chippet på framsidan. Kontaktlös betalning kategoriseras också som en CP-transaktion (Montague 2010 s. x). Ett exempel på en CP-korttransaktion är när kortinnehavaren sätter in kortet i betalningsterminalen vid kassan och trycker in sin PIN-kod.

2.3.2 CNP-transaktioner

Ifall kortet eller kortinnehavaren inte är fysiskt närvarande då transaktionen görs kategoriseras transaktionen som card-not-present (CNP). CNP-transaktionen sker då kortinnehavaren delar den synliga delen av informationen från kortet via internet, telefon eller e-mail för att göra ett köp (Montague 2010 s. x). Ett exempel på en CNP-transaktion är då kortinnehavaren beställer flyg på nätet och fyller in kortuppgifterna på nätsidan.

Skillnaden på de två korttransaktionerna är alltså närvaron av det fysiska betalningskortet. I denna studie fokuserar vi på kortbedrägerier där kortet inte är närvarande, dvs. CNP-korttransaktioner.

2.4 Betalningsprocessen

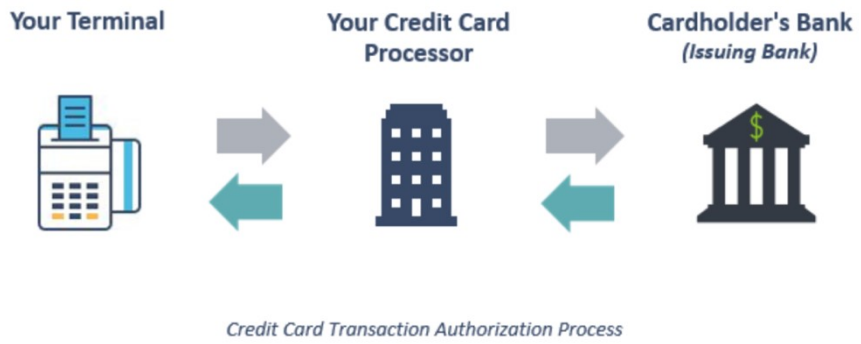
Hur kortbetalningar egentligen fungerar är något som de flesta inte tänker på när de står vid matbutikens kassa eller alternativt när de handlar kläder på nätet. Denna del framför hur betalningsprocessen ser ut och hur pengarna rör sig. Processen är väsentlig och mycket viktigt att förstå, för att senare kunna studera de själva kortbedrägerierna.

Före betalkortens tid i samhället behövde näringsidkarna inte verifiera vem konsumenten egentligen var när de tog emot betalningar för varor ifrån konsumenten. Näringsidkarna behövde inte heller oroa sig för att banken skulle komma till affären och kräva pengarna tillbaka för en försäljning. Det enda som näringsidkaren egentligen behövde verifiera vid köptillfälle var att pengarna hen tog emot räcker till för köpet och att pengarna inte är förfalskade. Det fanns helt enkelt bara två parter i kedjan, konsumenten och näringsidkaren. Processen förändrades i och med att nätbutiker och betalkort blev populära (Montague 2010, s. 38).

När betalkort kom in i bilden så förändrades situationen. Transaktionen som förut var mellan två parter, involverade nu i stället flera parter som till exempel näringsidkare, konsumenter, kortutfärdare, förvärvande banker, betalningsprocessorer och kortföreningar. Näringsidkarna kunde inte längre vid ett köptillfälle se om konsumenten har tillräckligt pengar för att genomföra inköpet, utan hamnade i stället lita på att de tredje parterna i kedjan ser till att konsumenten för det första är auktoriserad för att slutföra inköpet och för det andra har råd med produkten (Montague 2010 s. 39).

2.4.1 Verifieringsprocessen

Det första steget vid ett inköp är verifieringsprocessen. Detta steg görs både när kortinnehavaren gör ett CNP-kortköp, samt när kortinnehavaren gör ett CP-kortköp. I följande exempel framförs hur verifieringsprocessen i ett CP-kortköp kan se ut. Stegen ser ungefär likadana ut oberoende om det är frågan om ett CNP- eller CP-kortköp. Den enda skillnaden i de två processerna är att det inte finns ett betalkort på plats vid ett CNP-kortköp, utan de synliga kortuppgifterna från betalkortet matas i stället manuellt in i en kortterminal eller en gateway tjänst (Dwyer 2020).

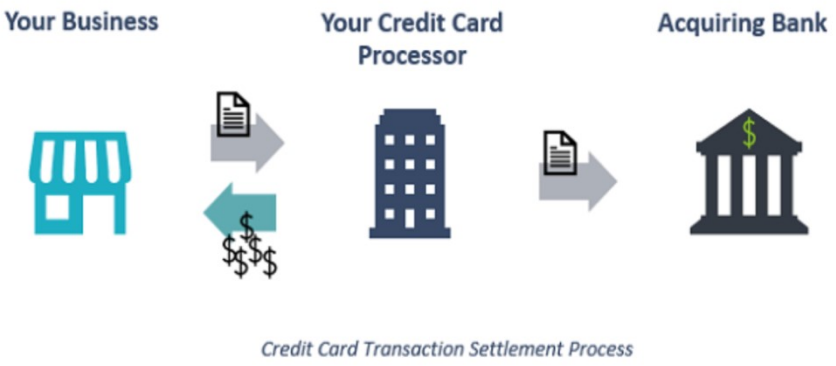


Figur 1 Verifieringsprocessen (Dwyer 2020)

En konsument placerar in sitt betalkort i näringsidkarens kortterminal. Näringsidkarens kortterminal skickar kortuppgifterna vidare till näringsidkarens bank, det vill säga förvärvande banken. Förvärvande banken skickar vidare kortuppgifterna till kortföreningen. Detta sker ofta via en betalnings processor. En betalnings processor är dock inte obligatorisk i processen. Kortföreningen granskar kortnumrets säkerhetsuppgifter och identifierar den rätta kortutfärdaren med hjälp av uppgifterna. Kortföreningen skickar kortuppgifterna vidare till den rätta kortutfärdaren antingen direkt eller via en betalnings processor. Kortutfärdaren verifierar att kunden har tillräckligt med pengar eller användbar kredit på sitt konto. Ifall det finns tillräckligt med pengar eller kredit på kundens konto, reserveras den totala summan för inköpet från konsumentens konto. Ifall det inte finns tillräckligt med pengar eller användbar kredit på kundens konto, kan reservationen för inköpet inte göras. Kortutfärdaren skickar efter det ett jakande eller nekande svar ända tillbaka till förvärvande banken som i sin tur för svaret vidare till näringsidkarens kortterminal. Ifall svaret är jakande går köpet igenom, ifall svaret är nekande ber kort-

terminalen konsumenten att försöka igen eller försöka slutföra inköpet med hjälp av ett annat betalmedel (Dwyer 2020).

2.4.2 Hur får näringsidkaren betalningen?



Figur 2 Clearing processen (Dwyer 2020)

För att näringsidkaren skall få betalt för produkterna hen sålt måste hen skicka en omgång med information om alla verifierade transaktioner till sin förvärvande bank. Omgången skickas oftast en gång per dygn. Förvärvande banken skickar transaktions detaljerna till kortföreningen antingen direkt eller via en betalnings processor. Kortföreningen ser till att informationen skickas vidare till rätt kortutfärdare. Kortföreningen för vidare transaktions detaljerna till kortutfärdaren antingen direkt eller via en betalnings processor. Kortutfärdaren krediterar den reserverade summan av konsumentens betalkort och för summan vidare till näringsidkarens förvärvande bank. Förvärvande banken överför summan vidare till näringsidkarens bankkonto. Ifall konsumenten har använt ett kreditkort vid köptillfället, skickar kortutfärdaren en räkning till konsumenten nästa månad med information och detaljer om inköpet som gjorts med konsumentens kreditkort. Ifall konsumenten har använt ett debetkort vid köptillfället, krediteras summan rakt från konsumentens bankkonto och konsumenten kan hitta information om inköpet som gjort i sin egen nätbank (Dwyer 2020, Nordea Bank Oyj. 2021).

2.5 Bedrägeri

För att samhället skall fungera och medlemmarna i samhället skall kunna känna sig trygga behöver samhället regler, det vill säga lager. Lagerna definierar vissa typer av beteende som oacceptabla, som brott. Brott har många olika former och varje form riktar sig mot en viss skada. Det finns brott som riktar sig att skada individer (till exempel misshandel, mord), egendom (till exempel bedrägeri, stöld) och miljö (till exempel nedskräpning). Eftersom samhällen har behövt hantera olika brott i årtusenden har de ut utvecklat standardiserade definitioner av de vanligaste brotten i samhället (Brenner 2012 s. 8).

Precis som med andra traditionella brott som stöld och utpressning är bedrägeri inte något nytt, men ändå något som blivit allt mera vanligt i dagens samhälle. Enligt polismyndigheten (2019) börjar bedrägerier i själva verket bli ett av de vanligaste brotten som folk råkar ut för. Bedrägeri beskrivs i lag om strafflagen som att erhålla en olaglig ekonomisk fördel för sig själv eller någon annan, skada någon annan genom att utnyttja ett fel, få en annan att göra eller underlåta att göra något och därmed orsaka ekonomisk skada för den som misstagit sig (Bergfors 2019, Finlex 24.8.1990/769).

I och med att världen förändras och blir mera digital förändras även sätten människor begår bedrägerier. Internet, e-post och sociala medier är bra exempel på ställen där digitaliseringen av världen har skapat nya plattformar för gärningsmän att begå traditionella brott som till exempel bedrägeri.

2.5.1 Internetbrott

Begreppet internetbrott omfattar i stort sett all brottslighet som sker eller utnyttjar internetet. Internetbrott skiljer sig från andra typer av brott främst i sättet det begås på. Då de traditionella brottslingarna på gatan använder sig av fysiska verktyg som till exempel vapen, för att begå sina brott, använder internetbrottslingar i stället datorteknik för att begå sina brott (Gottschalk 2010 s. 10).

Största delen av internetbrotten som vi ser i dagens samhälle representerar enligt Susan Brenner (2012) helt enkelt migrationen från gatorna till internet. Det vill säga internetet blir ett verktyg som brottslingar använder för att begå samma gamla brott som till exempel bedrägeri, stöld och utpressning, men på ett nytt sätt. Internetet har också gjort det möjligt för kriminella att nå en mycket bredare grupp av människor än förut och därmed förbättra resultatet av brottet. Där gärningsmannen förut fysiskt hamnade vara i någon slags kontakt med offret, kan hen nu i stället sitta vid en dator hemma, på ett bibliotek, i ett café eller någon annanstans. Gärningsmannen behöver nödvändigtvis inte ens befinna sig i samma land som offret (Brenner 2012 s. 8).

Internetbrott är också mycket svårare att utreda än traditionella brott. Det beror på att gärningsmannen inte fysiskt behöver vara på plats i en affär för att utföra brottet. Dessutom kan hen skydda sin identitet genom att dölja den eller helt enkelt använda någon annans. Internetbrott som till exempel CNP- kortbedrägerier, görs ofta på utländska nätsidor av personer som inte i själva verket har några kopplingar till offrets eller hens hemland (Brenner 2012 s. 13).

Eftersom brottet överskrider internationella gränser gör det utredandet av brottet väldigt svårt. Utredningen skulle i de flesta fall helt enkelt kräva för mycket tid och resurser i tanke på den potentiella belöningen, även om samarbetet mellan länderna skulle fungera på ett bra sätt. Samtidigt blir risken för att åka fast mindre. Brottet ses som lågt riskabelt, med en potentiellt hög belöning. Dessutom kan det räcka en lång tid för offret att i själva verket förstå vad som hänt. Om någon stjäl din plånbok på gatan, märker du antagligen det rätt så snabbt och då kan du spärra dina betalkort samt meddela polisen om vad som hänt. Gärningsmannen har även måsta befinna sig fysiskt på plats för att utföra brottet. Den finansiella skadan kommer antagligen inte heller bli så stor eftersom gärningsmannen har en ganska kort tid på sig att använda dina betalkort. (Brenner 2012 s. 9–13). Föreställ dig nu i stället att någon får tag på dina kortuppgifter på nätet. Skadan kommer i värsta fall upptäckas först nästa månad när du går igenom din kreditkortsfaktura. Dessutom är skadan antagligen betydligt större än om gärningsmannen har några timmar på sig att härja runt med ditt kreditkort, vilken hen i bästa fall inte en vet PIN-koden till.

Som tidigare nämnt så finns det olika typer av internetbrott och som tidigare nämnt, riktar sig varje brott till en viss skada. Internettbrott kan enligt Wells (2010) delas upp i kategorier. I vilken kategori brottet kategoriseras beror på sättet brottet görs, samt syftet med brottet. Alla internetbrott är inte i syfte vinstdrivna, det handlar i vissa fall också om till exempel sabotage. Exempel på sabotage är till exempel skadliga program eller hackning av webbsidor. Nedanför är ett exempel hur internetbrott delas upp i olika kategorier med underrubriker (Wells 2010 s. xvii).

1. Den första grenen innehåller brottstermer som hackning, cyberterrorism och sabotage. Denna gren innehåller internetbrott som till exempel virus, skadliga program, keyloggning, betala per klick manipulation, hackning av webbsidor, företagsspionage och utpressning.
2. Den andra grenen innehåller brott som investerings- och värdepapperstöld som till exempel ponzibedrägerier, obefintliga investeringar och marknadsmanipulation.
3. Den tredje grenen innehåller identitetsstölds brott. Som identitetsstöld anses bland annat stöld av personlig information, stöld av finansiell information och phishing.
4. Den fjärde grenen innehåller internet betalningsbedrägerier. Som betalningsbedrägerier anses bland annat checkbedrägerier, ogiltiga kredit- och debetkortnummer.
5. Den femte grenen innehåller konsumentbedrägerier. Konsumentbedrägerier kan till exempel vara löpande avgifter, skuldsanerings bedrägerier, välgörenhets bedrägerier, avgifter för tjänster som inte levereras.
6. Den sjätte grenen innehåller andra typer av internetbrott. Dessa internetbrott är till exempel korruption, penningtvätt och missbruk av tillgångar.

Även om CNP-kortbedrägerier placeras i den fjärde grenen är det inte alls ovanligt att kortbedragarna använder sig av brott som till exempel nämns i den tredje grenen av internettbrott för att först få tag på kortuppgifter. Därmed kombineras de olika grenarna i ett fall av kortbedrägeri.

I detta forskningsarbete jag mig på internetbrott i den fjärde grenen eftersom CNP-kortbedrägerier kan placeras där. CNP-kortbedrägerier är inte som ämne direkt svart och vitt och för att kunna täcka ämnet på ett korrekt sätt, måste arbetet även gå igenom andra internetbrott som hör ihop med ämnet. Dessa brott används för att få tag på kort-uppgifter eller för att förbättra resultatet (vinsten) i själva CNP-bedrägeriet. De olika sätten och taktikerna kortbedragarna använder sig av för att få tag på kortuppgifter tas upp senare i forskningen.

2.5.2 CNP-kortbedrägerier

CNP-kortbedrägerier är en from av internetbrott som satte i gång i mitten av 1990-talet när det blev möjligt att köpa varor från nätbutiker med betalkort. Företag var ivriga att få nätbutiker i stånd, för att kunna ta del av de nya möjligheterna. Med nya möjligheter kommer också nya hot och detta glömdes totalt bort i allt iver. Det tog inte en lång tid för kriminella att hitta på hur de kunde utnyttja företags splitternya nätbutiker för att i sin tur nå ekonomisk framskridande. I dagens läge kan man säga att förnyelsen tog går-dagens snattare till nästa nivå (Montague 2010 s. 61–63).

CNP-kortbedrägerier anses som ett ekonomiskt brott och är vinstdrivet. Som tidigare sagt, anses brottet lågt riskabelt med en potentiell hög belöning. Denna del av arbetet går igenom hur CNP-kortbedrägerier i dagens läge görs och jämför likheterna mellan processerna i identitetsstöld och betalkortbedrägeri.

Identitetsstöld och CNP-kortbedrägeri processerna har många likheter. De båda brotten är oftast internetbrott och i båda processerna försöker gärningsmannen få sig själv att se ut som någon hen inte är. Båda brotten görs med hjälp av offrets personliga uppgifter och uppgifterna används oftast för att nå ekonomiskt framskridande. Albrecht, Albrecht och Tzafrir (2011) beskriver identitetsstöld processen med tre olika steg.

Steg 1, gärningsmannen söker information om offret och verifierar att informationen stämmer. Detta kan till exempel göras så att gärningsmannen ringer upp offret och låtsas vara bankpersonal, en polis eller annat. Gärningsmannen hör helt enkelt av om den in-formation han fått ihop stämmer. Informationen som verifieras kan till exempel vara

hemadress, personnummer eller annat (Albrecht, Albrecht & Tzafrir 2011 s. 406–407, 409).

Steg 2, gärningsmannen förbereder verktyg i offrets namn som hen kommer att behöva för nästa steg. Verktyg kan till exempel vara kreditkort och körkort. Det andra steget innehåller också döljande av de spår som har skapats i identitetsstöld processen. Det kan till exempel handla om ringa banken och byta offrets telefonnummer, e-postadress eller hemadress. Detta görs för att offret inte skall få någon information om att hen har blivit utsatt för identitetsstöld (Albrecht, Albrecht & Tzafrir 2011 s. 407).

Steg 3, gärningsmannen börjar använda informationen och verktygen hen samlat för att få ekonomisk framskridande. Steg 3 börjar med att gärningsmannen gör små inköp där chansen att åka fast är liten. Ifall allt går bra ur gärningsmannens synvinkel, växer operationen och inköpen samt annat som görs i offrets namn växer (Albrecht, Albrecht & Tzafrir 2011 s. 407–408).

Teorin kan man bra applicera för CNP-bedrägerier eftersom, brotten samt förberedelserna är i många fall liknande. Hur stegen appliceras för CNP-bedrägerier förklaras till näst.

Steg 1, CNP-bedrägeri processen börjar med att söka informations likasom i identitetsstöld processen. Steget är väldigt viktigt eftersom hela processen beror på detta steg. Den information som gärningsmannen minst behöver om offret för att gå vidare till nästa steg i processen är kortnummer, utgångsdatum, CVV-kod och kortinnehavarens namn. Ifall gärningsmannen har fått tag på offrets nätbankskoder är det ett stort plus för gärningsmannen, eftersom flera europeiska nätbutiker i dagens läge ber kunden identifiera sig när de gör ett inköp (Montague 2010 s. 57–59).

Steg 2, gärningsmannen verifierar att kortuppgifterna stämmer. Det kan till exempel göras genom att mata in kortnumret när man registrerar sig själv som kund på en nätbutik. Ifall nätbutiken godkänner registreringen är kortet i bruk och fungerande. Verifieringen kan också göras genom ett köp på nätet. Summan för köpet är ofta under 10€. Ifall kortnumret fungerar är steget klart och gärningsmannen har ett fungerande kortnummer som

hen kan använda i nästa steg. Ifall kortnumret inte fungerar, måste gärningsmannen börja om från steg 1 (Montague 2010 s. 57–59).

Steg 3, gärningsmannen gör inköp med kort informationen hen i föregående steg har fått tag på och verifierat. Syftet med inköpen är som tidigare sagt, ekonomiskt framskridande och varorna som köps följer ofta syftet. Tanken är att antingen sälja varorna som beställts eller själv ta dem i bruk. Inköpen görs ofta i en snabb takt för att undvika att kortinnehavaren eller banken förstår vad som pågår. Ifall kortinnehavaren inte märker vad som har skett, kan gärningsmannen antingen fortsätta använda kortet eller sälja vidare kortuppgifterna till nästa gärningsman (Montague 2010 s. 57–59).

2.6 Kortuppgifter

För att begå CNP-kortbedrägerier behöver gärningsmannen kortuppgifter. Kortuppgifterna som behövs för att göra inköp på nätet är i minsta fall kortnumret, kortinnehavarens namn och utgångsdatumet (Brex 2021). De flesta europeiska nätbutiker kräver vid ett inköp även idag CVV-kod. Finska och andra nordiska nätbutiker har nyligen även börjat kräva att kunden identifierar sig med hjälp av nätbankskoder för att undvika CNP-bedrägerier. Även om säkerheten kring CNP-inköp, samt lagstiftning i Norden och övriga Europa har tagit ett framsteg i bekämpning mot CNP-kortbedrägerier begås det dagligen flertal kortbedrägerier även här i Norden.

För att få tag på kortuppgifterna som behövdes för att göra CNP-kortbedrägerier använde gärningsmän sig i början sig av stulna betalkort. Korten kunde stjälas antingen fysiskt från kortinnehavaren eller så kopierade gärningsmännen betalkortet (skimming). Skimming används även i dagens läge, med syfte att skapa fysiska kortkopior som sedan kan användas för att lyfta kontanter.

Andra historiska trender som användes för att få tag på kortuppgifter var att stjäla post och sopdykning. När man stal post försökte man känna på kuvert för att få reda på om det innehöll ett betalkort som skickats från kortutfärdaren. Sopdykning handlade i stället om att försöka hitta gamla betalkort vars giltighetstid hade gått ut. Den enda informationen som förändras i jämförelse med det föråldrade betalkortet, till det nya, är giltig-

hetstiden och eftersom månaden hålls den samma, så var det inte speciellt svårt att gissa sig fram till det korrekta åratalet som stod på det nya betalkortet (Montague 2010 s. 62–63)

Man förstod snabbt riskerna och insåg att dessa trender inte var speciellt effektiva. I stället uppstod nya, bättre sätt att få tag på kortuppgifterna gärningsmännen behövde. Nästa trend som gärningsmännen kom på var att själv grunda falska nätbutiker. Gärningsmännen samlade ihop kortuppgifterna och ”sålde” varor till kunderna som beställde varor på nätsidan. Efter att gärningsmännen fått ihop en fin summa, och en massa kortuppgifter stängde de ner nätbutiken och började använda kortuppgifterna för att själv nå en ekonomisk framgång (Montague 2010 s. 63–64).

I dagens läge försöker gärningsmännen få tag på kortuppgifterna utan att offret vet eller förstår det. Vissa gamla trender, som till exempel falska nätsidor, finns kvar även i dagens läge. De huvudsakliga metoderna som i dagens läge används för att få tag på kortuppgifter är dock phishing, dataintrång, och Tor-nätet. I nästa avsnitt förklaras metoderna närmare.

2.6.1 Phishing

Phishing, eller nätfiske, går ut på att gärningsmän försöker få ut känslig information som till exempel kortuppgifter, nätbankskoder eller annat genom att utge sig vara någon annan än hen i själva verket är. Ofta handlar det om att gärningsmannen företräder som bankpersonal, polis eller en person i en annan pålitlig ställning för att lura eller manipulerar offret.

Phishing kan begås via till exempel e-mail, textmeddelanden eller telefonsamtal. Innehållet på textmeddelandena eller e-mejlen varierar till stor grad, men slutresultatet är oftast samma, gärningsmannen försöker manipulera offret att dela med sig de känsliga uppgifterna eller informationen (Capgemini 2012 s. 7, Daly 2020).

2.6.2 Dataintrång

Dataintrång är ett annat sätt att få tag på kortuppgifter. Dataintrång innebär att man utnyttjar svagheter i säkerheten och tränger sig in i datorsystem eller nätverk för att få tag på känslig information som till exempel kortuppgifter. Gärningsmannen kan sedan själv utnyttja informationen eller sälja den vidare till tredje parter (Daly 2020).

2.6.3 Tor-nätet

Efter att kortuppgifter har stulits via till exempel ett dataintrång kan gärningsmannen sälja kortuppgifterna hen fått tag på ifall hen så väljer. Kortuppgifterna kan såklart inte säljas på öppna marknaden eftersom polisen eller andra oönskade parter därmed kan få reda på aktiviteten. I stället har det skapats så kallade ”carding forum”.

Carding forum är webbplatser i Tor-nätet där man kan utbyta information och teknisk kunskap, samt köpa och sälja bland annat stulna betalkortsuppgifter, nätbankskoder, personnummer och förfalskade valutor. Priset gärningsmannen kan be för kortuppgifter beror på hur mycket kortuppgifter dataintrånget har resultera i, samt kvalitén på kortuppgifterna. Kvalitén betyder i detta sammanhang kortuppgifternas validitet, samt annan information som man fått under dataintrånget. Annan information kan till exempel stå för kortinnehavarens namn, adress, kortens CVV-koder och giltighetstider.

För att minimera risken att åka fast, bli spårad eller att bli igenkänd för dessa aktiviteter, sker betalningen för tjänsterna med hjälp av kryptovalutor (Chen 2020, Daly 2020).

2.7 Verktyg för bedrägerihantering

Det finns tre kategorier av kundkategorier som köper verktyg för att hantera bedrägerier. Den första kategorin innehåller näringsidkare, det vill säga företag med nätbutiker. Den andra kategorin innehåller betaltjänstleverantörer. Den tredje kategorin innehåller finansiella institutioner, såsom till exempel banker (Montague 2010 s. 111).

Den tredje kundkategorin är den absolut största kategorin, eftersom mera än nittio procent av finansiella institutioner utnyttjar något slags verktyg för att hantera bedrägerier

(Montague 2010 s. 111). Detta kapitel presenterar verktyg eller strategier, som banker kan använda för att förhindra kortbedrägerier, inklusive CNP-kortbedrägerier. Alla processer kan implementeras i till exempel, verifieringsprocessen eller clearing processen, utom CPP analysen som sker efter att ett kortbedrägeri har tagit plats (Holmes 2021).

2.7.1 Transaktionsmonitorering

Transaktionsmonitorering anses vara ett av de viktigaste verktygen för finansiella institutioner och är enligt Montague (2010) ett måsta på för banker. Transaktionsmonitorering kan användas på flera olika avdelningar i banker. Dessa avdelningar kan till exempel vara, bedrägeriavdelningen, penningtvättavdelningen och sanktionsavdelningen. Transaktionsmonitorering går ut på att i real tid granska transaktioner som görs, och stoppa de transaktionerna som kan anses misstänksamma. När en transaktion stoppas, flaggas transaktionen. De flesta banker har automatiserat processen (Montague 2010 s. 122, Bristow 2021).

2.7.2 Regler

Banker använder så kallade regler för att stoppa och flagga transaktioner som görs av de kriminella. Reglerna programmeras på basen av transaktioner som har upptäckts, till exempel i transaktionsmonitoreringen, och visat sig vara bedrägliga. Reglerna formas av variabler som koncentrerar sig på transaktionens egenskaper. Dessa kan till exempel vara transaktionens summa, valuta, geografiska plats eller annat. Regler måste uppdateras manuellt efter de hotbilder som upptäckts i verksamheten (Capgemini 2012 s. 12).

2.7.3 Listor (Heta, varma, positiva)

Listor innehåller till exempel, kortnummer, försäljarnummer, terminalnummer eller andra specificerande nummerkoder. Listorna används av finansiella institutioner, försäljare och andra företag för att markera bedrägliga kunder, dåliga kunder och bra kunder. Banker kan till exempel använda heta listor för att flagga korttransaktioner från en specifik försäljare, som tidigare har visat sig vara bedrägliga. Banker kan också använda listor för att markera kortnummer som tidigare har utsatts för bedrägliga transaktioner (Montague 2010 s. 199–200, Fraudpractice.com 2020)

2.7.4 CPP analys

CPP analys är ett viktigt steg i det förebyggande arbetet av CNP-kortbedrägerier. CPP analysen går ut på att hitta stället varifrån kortuppgifterna som de kriminella har använt härstammar, det vill säga varifrån kortuppgifterna har fåtts. När man utför en CPP analys använder man information och data som fåtts från kort som redan har använts bedrägligt. Det är alltså frågan om att hitta stället i korthistoriken där det har begåtts ett dataintrång. Att hitta platsen varifrån kortuppgifterna härstammar kan ofta vara svårt eftersom kortuppgifterna säljs vidare till tredje personer och dessutom ofta sorteras till olika portfolion med kortuppgifter. Detta innebär att kortuppgifter som fåtts i samma dataintrång ofta inte används vid samma, eller närliggande tillfälle. Detta är en sorts säkerhetsåtgärd från de kriminellas sida, som försöker komplicera, eller göra bankernas jobb svårare. CPP analyser kan göras manuellt men enligt Holmes (2021) lönar det sig att automatisera arbetet åtminstone till någon grad (Holmes 2021).

3 METOD

I denna del av arbetet presenterar jag olika forskningsmetoder, samt redogör vilken forskningsmetod jag valt och varför. Efter att metodvalet är presenterat, framför jag tillvägagångsättet och urvalsmetoden.

3.1 Forskningsmetoder

Forskningsmetoden i ett examensarbete är ett verktyg som används för att hitta svar eller förklara och förstå ett problem, en uppläggning eller strategi för att få kunskap om ämnet.

Forskningsmetoder kan delas in i två huvudkategorier, kvalitativ och kvantitativ. Båda huvudkategorierna är stödda av tjocka och komplexa litteraturer och både och ger användbara och informativa resultat när de utförs väl (Davies & Hughes 2014 s. 9).

Även om huvudkategorierna har sina likheter så tjänar de i slutändan olika syften och vilken av huvudkategorierna man väljer för sin studie, beror på sättet syftet, forskningsproblemet och forskningsfrågorna definieras (Davies & Hughes 2014 s. 23–24).

Vissa hävdar också att det inte är en fråga om vilken väg de skall gå när det gäller kvalitativa eller kvantitativa metoder, utan vilken sorts kunskap de i slutändan vill generera (Davies & Hughes 2014 s. 9).

3.1.1 Kvantitativ forskningsmetod

Kvantitativ forskning kan beskrivas som en deduktiv forskningsstrategi som vid datainsamlingen och analysen betonar siffror, volymer och kategorier, snarare än ord eller bilder (Bryman 2012 s. 160). Därför är en kvantitativ forskning ofta mer storskalig, jämfört med en kvalitativ forskning. (Davies & Hughes 2014 s. 9)

En kvantitativ forskning är till skillnad av en kvalitativ forskning, väldigt strukturerad och forskaren skall hålla sig neutral i studien. Urvalet i forskningen skall vara representativt, det vill säga, urvalet skall ge information om hela helheten som studeras. (Davies & Hughes 2014 s. 9)

Kvantitativa forskningsmetoder kräver en noggrann problemformulering och data samlas ofta in genom enkätundersökningar, experiment eller dylikt. Data som insamlas skall vara kvantifierbar och resultaten analyseras med hjälp av till exempel statistikprogram som SPSS, för att göra slutsatser (Bryman 2012 s. 330)

Kvantitativ forskning lägger tonvikten på att testa teorier och kräver vanligtvis fler antal respondenter för att man skall kunna göra slutsatser om en teori kan generaliseras för en population eller inte (Bryman 2012 s. 330).

Datainsamlingsmetoder i kvantitativ forskning, sådana forskningar som använder fråge enkäter i synnerhet, kritiseras ibland för att dessa inte framför exakta resultat. Kritikerna menar att man inte kan vara säker på att respondenterna har tillräckligt med kunskap om ämnet som studeras för att svara på enkäterna. Dessutom påpekas det även att man inte kan veta hur resultaten korrelerar till respondenternas vardagsliv. Det kan alltså hända att respondenterna besvarar enkäterna på ett sätt, men i själva verket, agerar på ett motsatt sätt (Bryman 2012 s. 179).

3.1.2 Kvalitativ forskningsmetod

Kvalitativ forskning kan beskrivas som en induktiv forskningsstrategi som vanligtvis betonar ord, snarare än siffror och kategorier, vid insamling och analys av data (Bryman 2012 s. 380). Data som används i en kvalitativ forskning samlas oftast in via intervjuer, panelintervjuer, fallstudier eller enkäter med öppna svar (Christensen et al. 2001 s. 164–165). Tonvikten i en kvalitativ forskning läggs snarare på att generera nya teorier än att testa existerande teorier (Davies & Hughes 2014 s. 9).

Till skillnad från kvantitativa forskningsmetoder är syftet i kvalitativ forskning att beskriva ett fenomen, snarare än att mäta det (Davies & Hughes 2014 s. 9). Urvalsstorleken i en kvalitativ forskning spelar inte en lika stor skillnad, i jämförelse med en kvantitativ forskning. Antalet respondenter kan även ändras under studiens gång.

Kvalitativa forskningsmetoder är mer flexibla, i jämförelse med kvantitativa forskningsmetoder. Detta betyder att forskaren har en aning mera val när man jämför med datainsamlingsmetoder som till exempel intervjuer. Tillvägagångssättet i en kvalitativ forskning tenderar också att vara mycket mindre strukturerat än i en kvantitativ forskning (Bryman 2012 s. 470). Fokusen i en kvalitativ intervju, läggs på respondenten snarare än forskarens frågor. Ibland händer det att kvalitativa forskningar blir kritiserade. Detta beror på att dessa anses vara för subjektiva. Kritikerna menar att resultaten i studierna ibland speglar allt för mycket på vad själva forskaren, som utfört den kvalitativa studien, tycker att är betydelsefullt och viktig. Dessutom kritiseras det att kvalitativa forskare ofta har, eller formar en allt för nära personlig relation med respondenterna (Bryman 2012 s. 405).

3.2 Metodval

I denna forskning kommer jag att använda mig av en kvalitativ forskningsmetod eftersom syftet med studien inte är att mäta ett fenomen, utan att presentera vad bankerna kan göra för att bekämpa bedrägliga CNP-betalkortstransaktioner samt försök till dessa.

En av de populäraste datainsamlingsmetoderna inom kvalitativ forskning är intervjuer. Intervjuer är ett bra och effektivt sätt att få åsikter, en helhetsbild och nå en god reliabi-

litet om hur personer ser på ämnet som studeras. Intervjuerna tenderar att vara mer flexibla jämfört med kvantitativa intervjuer vilket gynnar mig eftersom jag vill fråga följdfrågor och skapa en dialog med respondenterna. Detta torde resultera i att data som utfås i intervjuerna motsvarar verkligheten något närmare (Bryman 2012 s. 470).

I en kvalitativ intervju läggs tonvikten på respondentens perspektiv på ämnet som studeras, det vill säga, forskares intresse för intervjupersonens synvinkel och åsikter är mycket större än i en kvantitativ intervju, vilket också gynnar mig i genomföringen av min studie (Bryman 2012 s. 470).

För att åstadkomma det bästa resultatet finns olika sätt och tekniker att utföra intervjuerna. De intervjuade kan vara enskilda eller i grupp och de själva intervjuarna kan också variera i nummer (Simonsson, Hjorth, Sandberg & Thelander 1998). I denna studie kommer jag att använda mig av kvalitativa semistrukturerade intervjuer med personer som arbetat i finansbranschen under en längre tidpunkt och kan anses vara specialister inom ämnet som studeras.

3.2.1 Kvalitativ semistrukturerad intervju

Semistrukturerad intervju är den datainsamlingsmetod som används för att samla in data om ämnet som studeras. En semistrukturerad intervju kan fungera som den enda datainsamlingsmetoden i en forskning eller så kan den kombineras med en annan datainsamlingsmetod för att forma en så kallad hybrid modell. I detta arbete används den som den enda insamlingsmetoden och kombineras med en så kallad intervjuguide (Galletta 2013 kapitel 12).

Datainsamlingsmetoden i fråga, är tillräckligt strukturerad för att man skall kunna framföra specifika områden eller processer som är relaterade till ämnet som studeras, men erbjuder samtidigt utrymme för deltagarna att uttrycka sig (Galletta 2013 kapitel 12).

En semistrukturerad intervju fungerar bra fast forskningsämnet som studeras är komplext, eftersom skribenten kan engagera sig och bland annat, ställa följdfrågor. Metoden är alltså flexibel både för respondenten och för skribenten (Galletta 2013 kapitel 12).

För att en semistrukturerad intervju skall lyckas och intervjun skall framskrida bra, måste man förbereda och formulera intervjuguiden och frågorna som ställs i intervjun på ett korrekt sätt. Frågorna kan vara öppna eller så kan de vara mera strukturerade. Man kan även använda en hybrid av dessa. Skribenten kan också välja att byta ordningen på frågorna eller formulera frågorna på ett annat sätt ifall hen tycker situationen kräver detta (Galletta 2013 kapitel 12).

3.3 Urvalsmetod

För att få den bästa möjliga data insamlat i intervjuerna, är det väldigt viktigt att respondenterna som används i intervjuerna har en hög kunskap och erfarenhet inom ämnet som studeras. Därför har jag beslutat att använda ändamålsenligt urval som urvalsmetod för detta arbete.

Ändamålsenligt urval går ut på att forskaren bedömer och väljer ut de respondenterna som skall användas i studien. Valen görs med tanke på vem som bäst kan besvara forskningsfrågorna i studien. Antalet respondenter som väljs i urvalet är ofta väldigt litet, eftersom tanken med urvalsmetoden är att välja de respondenter som förhoppningsvis kommer att vara de allra mest informativa i tanke på ämnet som studeras (Cassell, Cunliffe & Grandy 2017, kapitel 39)

I denna studie har jag att skickat en förfrågan till sammanlagt 3 respondenter som jag personligen har valt ut. Valen som gjorts, grundar sig på deras erfarenhet och kunskap inom ämnet som studeras.

3.4 Tillvägagångssätt

I den empiriska delen av detta arbete kommer jag att utföra sammanlagt 3 intervjuer med personer som under en länge tidsperiod arbetat i finansbranschen. I själva intervjuerna använder jag mig av en intervjuguide (bilaga 1). Datat som samlats in i intervjuerna kommer att analyseras med hjälp av innehållsanalys.

Intervjuerna spelas in på en mobiltelefon och transkriberas inom 48 timmar efter att intervjuerna tagit plats. När transkriberingen är klar, raderas ljudfilerna. Efter att data som

fåtts i intervjuerna är bearbetad och analyserad, raderas transkriberingen för att säkra respondenternas sekretess.

3.5 Reliabilitet

Validiteten och reliabiliteten av data som insamlats kommer påverkas av tiden som passerar. Resultaten som framförs i studien kommer att förändras över tid eftersom processer förändras, utvecklas och förbättras. Det betyder att det resultatet som idag fås ut, inte nödvändigtvis stämmer över en längre tidsperiod. Data som fås i intervjuerna kan ändå anses vara valid för denna, samt närliggande tidpunkt.

4 RESULTATET AV DEN EMPIRISKA DELEN AV ARBETET

I detta kapitel presenteras resultaten av intervjuerna via en granskning av respondenternas erfarenheter och synvinklar om hur banker kan bekämpa bedrägliga CNP-betalkortstransaktioner samt försök till dessa.

Jag genomförde kvalitativt semistrukturerade intervjuer med tre personer. Alla tre personer har arbetat på finansbranschen under en längre tidsperiod och kan anses vara specialister inom ämnet i fråga. Två av intervjuerna utfördes i ett mötesrum på skribentens arbetsplats, medan den sista intervjun utfördes hemma hos skribenten. Intervjuerna med respondenterna räckte i snitt mellan ca. 40–55 minuter. Intervjuerna utfördes på finska och citaten som representerar respondenternas svar, kommentarer och åsikter har översatts till svenska.

De tre respondenterna i denna studie har döpts om, det vill säga, de får kodnamn: Respondent 1, Respondent 2, Respondent 3. Detta har gjorts i syfte att citera svaren och kommentarerna de intervjuade har framfört i intervjuerna.

De mottagna svaren och kommentarerna från deltagarna är indelade i tre huvudkategorier som fastställts genom att transkribera de inspelade intervjuerna. Den första kategorin består av bakgrundsfrågor gällande CNP-kortbedrägeri. Den andra kategorin fokuserar sig på det förhindrande arbetet som görs i realtid när bedrägliga transaktioner upp-

täckts, samt processen efter att kortbedrägeriet har upptäckts. Den tredje kategorin fokuserar sig på det förebyggande arbetet som görs för att förebygga möjliga kortbedrägerier. Tillsammans bildar dessa kategorier en helhetsbild om ämnet som studeras.

Kategori 1: *Bakgrundsfrågor om CNP-kortbedrägerier*
Kategori 2: *Förhindrande arbete av CNP-kortbedrägerier*
Kategori 3: *Förebyggande arbete av CNP-kortbedrägerier*

4.1 Bakgrundsfrågor om CNP-kortbedrägeri

Jag började med att ställa frågor till respondenterna generellt om kortbedrägeri, eftersom jag ville veta hurdan deras uppfattning och erfarenhet om ämnet är. Jag började intervjuerna med att fråga respondenterna vad kortbedrägeri är. Det fanns ingen märkvärdig variation i svaren, utan alla var eniga om att det handlar om att använda någon annans betalkort eller kortuppgifter obehörigt för att skaffa sig pengar eller annan egendom.

Till näst frågade jag vad skillnaden är mellan kortbedrägeri och CNP-kortbedrägeri. Respondenterna svarade att CNP-kortbedrägeri är en slags form av kortbedrägeri. Skillnaden är endast att betalkortet inte är fysiskt på plats vid ett CNP-kortbedrägeri.
Nästa fråga jag ställde var hur vanliga CNP-kortbedrägerier är i dagens samhälle. Respondenterna var även eniga om att dessa kan anses väldigt vanliga i dagens samhälle. Variationen i svaren blev dock större när jag frågade respondenterna om de tror att antalet CNP-kortbedrägerier kommer att växa i framtiden. Två respondenter svarade ja medan en sa att hen tror att dessa varken kommer växa eller sjunka i antal. Respondenterna är ändå eniga om att det troligen inte handlar om en radikal förändring i antal. Respondenterna svarade följandevis:

”Världen blir ju alltmer digital dag för dag så dom kommer nog växa, inte nödvändigtvis radikalt men iallafall.” (Respondent 2)

”Historian visar att antalet stiger år för år och jag tror inte att det kommer att ske någon ändring i det.” (Respondent 3)

”Antalet kommer antagligen inte vare sig växa eller sjunka dramatiskt. Antalet kommer nog hållas rätt så stadigt i när framtiden skulle jag satsa på.” (Respondent 1)

Till näst frågade jag respondenterna om varifrån de kriminella får tag på kortuppgifterna för att utföra CNP-kortbedrägerier. Respondenterna lyfte fram dataintrång, phishing och Tor-nätets carding forum som de tre vanligaste källorna. En av respondenterna svarade på följandevis:

”I dagens läge utförs oftast ett dataintrång och kortuppgifterna används sedan själv eller så säljer man dem vidare på Tor-nätet… Phishing email är väldigt vanliga också.” (Respondent 1)

Respondenterna frågades sedan vems arbetsuppgift på banken det är att förhindra och förebygga CNP-kortbedrägerier. Respondenterna var eniga om att det antingen finns ett transaktionsmonitorerings team som antingen arbetar på banken eller är outsourcat. En respondent påpekade även följande:

”Arbetsuppgifterna kan även vara uppdelade så att ett team ansvarar över det förhindrande arbetet och ett annat team som består av analytiker ansvarar över det förebyggande arbetet av CNP-kortbedrägerier...” (Respondent 1)

4.2 Förhindrande arbete av CNP-kortbedrägerier

Till näst frågade jag respondenterna om det arbetet som görs på banker för att förhindra dessa CNP-kortbedrägerier. Jag ställde frågor om vad arbetet egentligen handlar om och hur de skulle definiera det. Respondenterna var eniga om att det förhindrande arbetet i stort sett handlar om transaktionsmonitorering. Två av respondenterna svarade på följandevis:

”Det förhindrande arbetet av CNP-kortbedrägerier görs inom transaktionsmonitoreringen. Man försöker för det första finna de bedrägliga transaktionerna när de själva transaktionerna görs och för det andra, att sätta stopp på dem”. (Respondent 3)

”För att förhindra CNP-kortbedrägeri använder banker transaktionsmonitorering. Men som sagt behöver själva transaktionsmonitoreringen inte nödvändigtvis ske i banken, utan processen kan även outsourcas till ett annat företag.” (Respondent 1)

Som följdfråga frågade jag vad transaktionsmonitorering som term betyder och innebär. Respondenterna förklarade att transaktionsmonitorering är en process som handlar om att övervaka korttransaktioner och upptäcka avvikande, möjligtvis bedrägliga korttransaktioner på kortinnehavarnas kort. Två av respondenterna svarade på följandevis:

”Transaktionsmonitorering betyder egentligen övervakning av transaktioner, i detta fall korttransaktioner ... Det finns också transaktionsmonitorering för bland annat penningtvätt.” (Respondent 2)

”Man övervakar kortinnehavarnas korttransaktioner för att upptäcka korttransaktioner som inte är gjorda av kortinnehavaren själv.” (Respondent 1)

Till näst gick jag djupare in på själva transaktionsmonitoreringen för att få veta hurdana processer banker har för att hitta dessa bedrägliga korttransaktioner bland enorma volymer av data. Respondenterna var eniga om att transaktionsmonitoreringen görs manuellt men att banker ofta använder datorsystem och både oövervakad samt övervakad maskininlärning, när det handlar om stora mängder data. Respondenterna förklarade att när man använder datorsystem och maskininlärning på ett korrekt sätt kan man minimera den data som måste hanteras manuellt. Två av respondenterna svarade på följandevis:

”För att kunna göra jobbet effektivt, kan banker i dagens läge använda sig av maskininlärning som gör processen betydligt mycket lättare ... datasystemet hittar nålarna ur höstacken.” (Respondent 1)

”No det är omöjligt at manuellt gå igenom alla korttransaktioner som görs dagligen och därför används det olika datorsystem och maskininlärning, det är liksom ett verktyg i arbetet.” (Respondent 2)

Som följdfråga frågade jag hur maskininlärning i princip används i själva transaktionsmonitoreringen för att förhindra CNP-kortbedrägerier. Två av respondenterna svarade på följandevis:

”Maskininlärning används i datorsystemen så att de skall flagga de transaktionerna eller transaktionsmönster som anses suspekta.” (Respondent 2)

”Banker använder sig av oövervakad maskininlärning för att hitta mönster och avvikelser och sedan flagga dessa avvikande transaktioner … Banker använder sig också av övervakad maskininlärning, till exempel regler, som är skapade för att hitta specifika transaktioner enligt de variablerna man har bestämt och sedan flagga dessa.” (Respondent 1)

Som följdfråga frågade jag vems arbetsuppgift det är att sköta om maskininlärningen i det förhindrande arbetet. Det uppkom ingen större variation i svaren, utan respondenterna förklarade att det vanligtvis finns ett team eller i alla fall ett par personer som ansvarar för programmeringen. Det påpekades även att tjänsten kan köpas från ett annat företag. En av respondenten svarade på följandevis:

”Banker kan ha ett team som sköter programmeringen eller så outsourcas själva programmeringen till något annat företag vars uppgift det är att sköta om det. Enstaka regler är ganska simpla att programmera så det kan även vara så att någon från transaktionsmonitoreringen har ansvar om dem. Men det beror som sagt på vad man har kommit överens internt i organisationen…” (Respondent 1)

De nästa frågorna jag ställde till respondenterna gällde processerna som sker efter att datorsystemet har så sagt, ”hittat nålen ur höstacken” och flaggat en transaktion. Det fanns ingen märkvärdig varians i respondenternas svar, utan alla respondenter var eniga om att dessa flaggade transaktioner sedan måste gås igenom manuellt. En av respondenterna svarade på följandevis:

”Man går igenom de flaggade transaktionerna manuellt och gör sedan ett sista hands beslut ... alltså om transaktionen faktiskt skall granskas med kortinnehavaren.” (Respondent 3)

Som följdfråga frågade jag respondenterna vad som letas efter, eller om det fanns några speciella tecken och hur man vet om att det handlar just om en bedräglig CNP-korttransaktion. Respondenterna förklarade att det letas efter något som avviker från den normala kortanvändningen. Samtidigt framfördes det att det även kan sökas efter tecken om att korttransaktionen i själva verket är gjord av kortinnehavaren själv. En av respondenterna lyfte även fram kundkännedom som en faktor i beslutsgörandet. Två av respondenterna kommenterade på följandevis:

”Om ett betalkort aldrig förut har använts på spelsajter och plötsligt försöker någon spela med många hundra euro, så ser det ganska märkligt ut... Då lönar det sig antagligen att kontakta kortinnehavaren för att kolla upp om det verkligen är hen själv som försöker använda kortet.” (Respondent 1)

”... Man kan anse att arbetet har mycket att göra med kundkännedom... Man försöker ställa sig i kundens ställning och fråga sig om det här är något kunden skulle göra.” (Respondent 2)

”... Sen kan man också vända på frågan och fråga sig själv om det finns några tecken på att kortinnehavaren faktiskt skulle ha gjort inköpet själv... Har till exempel kortinnehavaren verifiera sig själv med hjälp av nätbankskoder i sammanband med inköpet?” (Respondent 1)

Respondenterna var eniga om att avvikelserna inte dock alltid behöver vara lika uppenbara, utan att det också kan handla om enbart en avvikande valuta, en avvikande nätbutik i ett annat land eller en lite större summa en vad kortinnehavaren normalt använder. Två av respondenterna sa även att det ibland kan handla om en magkänsla av att något inte stämmer. En respondent svarade på följandevis:

”Det kan dock i princip vara vad som helst... Ibland kan man gå igenom gamla bekräftade kortbedrägerifall och tänka att det inte egentligen fanns något konstigt som stack ut här men någon inuti sa att det här är värt att kolla upp... Det var något som bara inte stämde med köpbeteendet.” (Respondent 3)

En respondent påpekade att man även kan ha standardiserade guider eller instruktioner som måste följas i detta skede. När jag frågade respondenten om ett exempel på en guide svarade hen på följandevis:

”No det kan handla om att man måste följa steg för stegs instruktioner som är standardiserade i företaget... Är valutan euro? Gör i så fall så. Är summan denna eller större? Gör i så fall så. Bor kunden i utomlands? Gör i så fall så...” (Respondent 2)

Till näst frågades respondenterna vad som händer efter att man har gjort beslutet att granska en korttransaktion. Respondenterna var eniga om att själva kortet i det skedet skall tillfälligt spärras för att förhindra andra, möjligtvis följande, bedrägliga CNP-kortbedrägerier. En av respondenterna svarade på följandevis:

”Kortet måste i detta skede spärras för att undvika andra bedrägliga korttransaktioner som kan följa efter.” (Respondent 2)

Jag ställde respondenterna en följdfråga om hur kort spärrningen sker. Respondenterna förklarade att det beror på hurdana processer och datorsystem som används i banken. Processen kan vara antingen manuell eller automatiserad. En respondent svarade på följandevis:

”Det beror helt på hurdant datorsystem banken använder... En robot kan till exempel vara programmerad att sköta spärrningen i samband med att en person vill granska en transaktion, eller så kan det handla om en kort manuell process.” (Respondent 1)

Följande frågor behandlade processen som sker efter att kortet är spärrat. Respondenterna var eniga om att nästa steg är att kortinnehavaren kontaktas för att få bekräftat om det handlar om kortbedrägeri eller inte. Som följdfråga frågade jag hur detta sker och vems

arbetsuppgift det är. Respondenterna svarade att det beror på bankens interna processer och regler. En respondent svarade på följandevis:

”Det beror på banken och hur man har kommit överens att processen sköts… Antingen kontaktas kortinnehavaren av transaktionsmonitorerings teamet eller kundservicen … Ifall transaktionsmonitoreringen är outsourcad till exempel utomlands är det antagligen så att kundservicen kontaktar kortinnehavaren.” (Respondent 1)

Respondenterna frågades sedan om hurdana kommunikationskanaler som används för att kontakta kortinnehavarna. Respondenterna förklarade att det beror helt och hållet på bankens egna processer. En respondent gav följande exempel:

”Kortinnehavaren kan kontaktas till exempel genom att ringa upp kunden, skicka SMS, skicka ett meddelande via nätbanken eller sen genom att skicka ett brev till kortinnehavarens hemadress.” (Respondent 2)

Respondenterna frågades till näst om vad som sker ifall transaktionen visar sig vara gjord av kortinnehavaren själv och vad som sker ifall kortinnehavaren inte känner igen korttransaktionen. Respondenterna förklarade att spärren avlägsnas ifall korttransaktioner visar sig vara gjord av kunden själv och ifall det visar sig vara frågan om en bedräglig korttransaktion så spärras kortet permanent och ett nytt kort med ett nytt kortnummer skickas till kunden. En respondent svarade på följandevis:

”Om det är korttinnehaven själv som försökt använda kortet avlägsnas spärren så klart … Om kortinnehavaren bekräftar att hen inte försökt använda kortet så skickas ett nytt kort till kortinnehavaren med ett nytt kortnummer. Gamla kortet skall också spärras permanent i så fall.” (Respondent 1)

En annan respondent påpekade även följande:

”… Möjliga ekonomiska förluster som uppstått på grund av att en tredje part har använt kortinnehavarens kortuppgifter utan lov, behöver inte kortinnehavaren ansvara för ifall hen inte har haft något med saken att göra.” (Respondent 2)

4.3 Förebyggande arbete av CNP-kortbedrägerier

De följande frågorna som ställdes till respondenterna behandlade det förebyggande arbetet av CNP-kortbedrägerier. Jag ställde frågor om vad arbetet egentligen går ut på. Respondenterna förklarade att arbetet går ut på att agera på basen av information som insamlats före det själva kortbedrägeri försöket tar plats. Två av respondenterna svarade på följandevis:

”Arbetet går ut på att samla och analysera data för att kunna agera innan de kriminella hinner använda kortuppgifterna de har fått tag på… Det är lite som att leka detektiv.” (Respondent 2)

”Det förbyggande arbetet spelar en avgörande del i att hantera CNP-kortbedrägerier. Man försöker samla in information och agera enligt den … Det handlar alltså av att vara proaktiv snarare än reaktiv.” (Respondent 1)

Som följdfråga frågades hurdan information som behövs för att utföra arbetet och varifrån den insamlas ifrån. Respondenterna förklarade att informationen som behövs för att utföra arbetet till stor del härstammar från bekräftade kortbedrägerier som upptäckts i transaktionsmonitoreringen. Informationen består av kortdata, det vill säga var någonstans kortet har använts och när. En av respondenterna svarade på följandevis:

”Informationen samlas in från kort som har upptäckts i transaktionsmonitoreringen … Informationen som används i det förebyggande arbetet består av kortdatan, det vill säga själva korthistorian på kortet.” (Respondent 1)

Följande frågor som ställdes till respondenterna gällde det insamlade kortdata. Respondenterna frågades vad som görs med kortdata och vad man letar efter. Respondenterna förklarade att man analyserar korthistorian för att hitta en så kallad CPP (Common Place of Purchase). När man hittat denna gemensamma faktor så kan man säkerställa var ett dataintrång har tagit plats. Två respondenter svarade på följandevis:

”Dessa insamlade data används för att försöka få fram en CPP… Utan en CPP kan man inte säkerställa källan varifrån kortuppgifterna har läckt … Alltså kan man inte utföra arbetet.” (Respondent 3)

”Kortdata analyseras för att hitta en CPP, alltså en plats i korthistorian där flera av korten som upptäckts i transaktionsmonitoreringen har använts vid ungefär samma tidpunkt. När man verifierat en CPP vet man var ett dataintrång har skett.” (Respondent 1)

Till näst frågades respondenterna om hur man går igenom kort data och ifall det är en automatiserad process eller inte. Två av respondenterna svarade att det finns företag som erbjuder datasystem som kan användas men att det förebyggande arbetet långt görs manuellt. Den tredje respondenten svarade att det förebyggande arbetet, till skillnad från det förhindrande arbetet, görs helt manuellt. En av respondenten svarade på följandevis:

”Kort data som insamlats kan gås igenom manuellt, men det tillverkas i dagens läge även datorsystem som är gjorda för att hitta likheter i kort data. Kortnumrorna matas in i datorsystemet och systemet letar sedan efter mönster och likheter i korthistorian.” (Respondent 1)

Respondent 1 påpekade dock att dessa datorsystem inte nödvändigtvis är det bästa verktyget för att finna en CPP eftersom systemet inte förstår att flera kortinnehavaren kan använda vissa företag månatligen. Respondenten använde Netflix, som fakturerar stora mängder av kortinnehavaren varje månad, som exempel. Respondenten kommenterade följande:

”Bara för att Netflix råkar debitera alla kort som matats in i datorsystemet, betyder det inte att företaget är CPP för korten… Det är bara en slump.” (Respondent 1)

Till näst frågades respondenterna om hur man listar ut en CPP. Respondenterna var eniga om att det kan vara svårt och att det ibland inte är möjligt att säkerställa en CPP. Respondenterna var eniga om att det krävs bevis för att fastställa en CPP. Beviset kan till exempel vara i form av flera kort, för att utesluta att det inte handlar om en slump.

Alltid är detta inte ens möjligt eftersom dataintrånget kanske bara resulterat i ett eller två av bankens kortnummer. Två av respondenterna förklarade följande:

”För att fastställa en CPP behövs bevis. Bevis kan till exempel vara fem kort som har använts på samma ställe under ungefär samma tidpunkt, varefter det har uppstått bedrägliga CNP-korttransaktioner på korten… Ibland är detta inte möjligt eftersom dataintrånget kanske bara resulterat i ett eller två av bankens kortnummer.” (Respondent 1)

”… Ibland lyckas man inte att hitta en CPP … Det kan till exempel bero på att dataintrånget endast har resulterat i ett av bankens kort eller så har kortinnehavaren råkat ut för phishing eller annat liknande.” (Respondent 2)

En av respondenterna påpekade även följande:

”… Visa och MasterCard skickar även listor med komprometterade kortnummer till banker efter att företag själva har upptäckt att det skett ett dataintrång i deras system.” (Respondent 2)

Som följdfråga frågade jag respondenten om hur många kortnummer det vanligtvis finns på dessa kortlistor. Respondenten svarade att det helt beror på var dataintrånget har skett och hur populärt företaget är bland konsumenterna. Respondenten kommenterade följande:

”Det kan handla om allt från ett eller två kortnummer upp till ett par hundra kortnummer, beroende på själva CPP.” (Respondent 2)

Till näst frågades respondenterna hur det själva förbyggande arbete utförs efter att man hittat en CPP. Respondenterna förklarade att efter man fastställt en CPP så måste det tas reda på hur många av bankens kort möjligtvis har komprometterats i dataintrånget och sedan måste korten spärras för att undvika att korten används i bedrägligt syfte. En av de intervjuade svarade på följandevis:

”Antalet kompromet terade kortnummer måste först tas reda på och sedan måste såklart korten spärras för att undvika att det skall uppstå bedrägliga korttransaktioner på kor-ten… Kortinnehavarna måste även kontaktas för att informera dem om att deras kort har kompromet terats och därför måste bytas ut.” (Respondent 3)

Som följdfråga frågades respondenterna hur processen av att spärra korten och kontakta kortinnehavarna genomförs. Respondenterna var eniga i att det beror på bankens interna processer. En av respondenterna svarade på följande vis:

”Generellt kan man säga att processen genomförs på ungefär samma sätt som i det fö-rebyggande arbetet… Hur processen exakt ser ut beror på banken och hur man har kommit överens.” (Respondent 2)

4.4 Analys

Denna del av arbetet fokuserar på att analysera svaren, erfarenheterna och åsikterna som respondenterna delat med sig i intervjuerna ovan. Respondenternas svar redogörs och tolkas, för att kunna göra slutsatser.

4.4.1 Transaktionsmonitorering

Under intervjuerna kom det fram att banker kan använda sig av transaktionsmonitore-ring för att hitta och förhindra bedrägliga CNP-korttransaktioner. Respondenterna berät-tade att transaktionsmonitoreringen går ut på att övervaka kortinnehavarnas korttrans-aktioner för att hitta avvikande transaktioner som möjligtvis är bedrägliga. Responden-terna påpekade att själva transaktionsmonitoreringen inte nödvändigtvis behövs göras i banken, utan att banker även kan outsourca arbetet till ett annat företag.

Respondenterna förklarade att man i transaktionsmonitoreringen letar efter transaktioner som avviker från kortinnehavarens normala kortanvändning. Man kan alltså säga att ar-betet handlar om kundkännedom, eftersom man måste veta hur kortinnehavaren van-ligtvis använder sitt kort. Avvikelserna som söks i transaktionsmonitoreringen behöver inte enligt respondenterna nödvändigtvis vara särskilt stora, utan det kan handla om en

avvikande valuta, summa eller nätbutik. En av respondenterna betonade att man även kan vända på saken och i stället leta efter tecken på att det i själva verket är kortinnehavaren själv som genomför korttransaktioner. Respondenterna påpekade att beslut ibland även görs med magkänsla.

I intervjuerna framkom det att banker även kan använda standardiserade guider i transaktionsmonitoreringen. I så fall har man steg för steg instruktioner som man följer för varje flaggad transaktion.

4.4.2 Datorsystem och maskininlärning

Det utförs miljontals korttransaktioner dagligen bara i Finland och att hitta de bedrägliga transaktionerna ifrån mängden är som en av respondenterna sa, ”som att hitta nålen ur höstacken”. Respondenterna förklarade att banker därför kan använda sig av datorsystem och maskininlärning vars uppgift det är att hitta och flagga de avvikande korttransaktionerna.

Banker kan använda sig av både oövervakad och övervakad maskininlärning i transaktionsmonitoreringen. Skillnaden på de övriga är att datorsystemet använder den data som matas till den för att lära sig själv när det handlar av oövervakad maskininlärning, medan man lär datorsystemet att välja rätt när det handlar om övervakad maskininlärning. Ett exempel på övervakad maskininlärning som banker kan använda sig av i transaktionsmonitoreringen är så kallade regler. Reglernas uppgift är att flagga korttransaktioner på basen av de variabler man har programmerat.

Dessa verktyg sparar tid och gör arbetet enklare för banker, eftersom datasystemet med hjälp av maskininlärning kan plocka fram de avvikande korttransaktionerna och personalen sedan kan fokusera sig på dem.

4.4.3 Insamling av data

I intervjuerna framkom det även att ett annat viktigt steg gällande det förebyggande arbetet görs i själva transaktionsmonitoreringen, nämligen datainsamling. I transaktions-

monitoreringen samlas det in all information om upptäckta CNP-kortbedrägerier samt försök till dessa. Informationen i fråga handlar om kortdata, det vill säga, information om var kortet används och när. Denna information kan sedan användas i det själva förebyggande arbetet.

Enligt respondenterna får banker även information om komprometterade kortnummer från tredje parter, till exempel Visa och MasterCard, som skickar listor som innehåller komprometterade kortnummer.

4.4.4 Dataanalys

Respondenterna förklarade att man i det förebyggande arbetet analyserar kortdata som insamlats i till exempel, transaktionsmonitoreringen. Kortdata analyseras med syfte att hitta den platsen där de kriminella fått tag på kortuppgifterna, det vill säga, för att finna platsen där det skett ett dataintrång. Analysen av kortdata kan enligt respondenterna göras både manuellt samt med hjälp av datorsystem, även om respondenternas personliga erfarenheter hävdar att det manuella sättet möjligen är bättre.

I kortdata försöker man hitta en så kallad CPP, som uttrycker var dataintrånget har skett. Ifall man hittar stället där dataintrånget tagit plats, försöker man ta reda på vilka kortnummer har använts på platsen under dataintrångets tidpunkt. Att hitta en CPP är dock inte alltid lätt och som respondenterna förklarade, hittas en sådan ibland inte över huvud taget.

4.4.5 Nytt betalkort

Vare sig det handlar om att förhindra eller förebygga CNP-kortbedrägerier, så hamnar banken alltid byta ut och spärra kortinnehavarens gamla kort för att se till att inga nya CNP-kortbedrägerier inträffar kortinnehavaren. Respondenterna förklarade i intervjuerna att kortförnyelse processen helt och hållet beror på vilken bank kortinnehavaren har, samt deras interna processer. Rent generellt kan man ändå enligt respondenterna säga att banken kommer att kontakta kortinnehavaren och berätta vad som sker även om processen kan se en aning annorlunda ut beroende på banken.

5 SLUTSATSER

I denna del av arbetet drar jag slutsatser av det förhindrande, samt förebyggande arbetet av CNP-kortbedrägerier på basen av analysen som gjorts i den tidigare delen av arbetet.

Respondenternas svar förstärker det som framkommit i teoridelen av arbetet. Man kan konstatera att transaktionsmonitorering är en väldigt viktig del av det förhindrande arbetet av CNP-kortbedrägerier. Transaktionsmonitoreringen kan antingen göras i banken eller så kan banken outsourca arbetet till ett annat företag. Transaktionsmonitoreringen går ut på att övervaka kortinnehavarnas korttransaktioner i syfte att upptäcka avvikande, möjligtvis bedrägliga korttransaktioner. Korttransaktionsvolymen är dock väldigt hög och för att hitta och flagga dessa bedrägliga korttransaktioner ur mängden, kan banker använda sig av hjälpmedel eller verktyg i form av datorsystem och maskininlärning. Idén med verktyg som datorsystem och maskininlärningen är att minimera den mängd korttransaktioner som måste gås igenom manuellt och därför kan man konstatera att effektivt och bra utförd programmering av datorsystem är en hörnsten i det själva förhindrande arbetet av CNP-kortbedrägerier.

I intervjuerna framkom det att korttransaktioner som datorsystemen har flaggat i transaktionsmonitoreringen, sedan gås manuellt i genom av transaktionsmonitorerings teamet. Personerna i teamet letar efter tecken som skulle kunna betyda att korttransaktionen inte är gjord av kortinnehavaren själv, eller på tecken att korttransaktionen faktiskt är gjord av kortinnehavaren själv. Respondenterna lyfte i intervjuerna fram kundkännedom som en viktig faktor i arbetet eftersom man måste förstå hur kortinnehavaren vanligen använder sitt kort. I intervjuerna påpekades dock att beslut i transaktionsmonitoreringen även ibland görs på magkänsla. Detta betyder att även erfarenhet om ämnet har en stor roll i det praktiska arbetet.

I intervjuerna framkom det att information som kan användas i det förebyggande arbetet samlas in i transaktionsmonitoreringen. Informationen i fråga fås från kort som drabbats av bedrägliga korttransaktioner och består av kortdata, det vill säga information om var någonstans kortuppgifterna har använts och vid vilken tidpunkt. Denna information används sedan i det förebyggande arbetet för att försöka hitta en så kallad CPP. Arbetet

som görs för att hitta en CPP, det vill säga CPP analysen kan anses vara den avgörande delen i det förebyggande arbetet eftersom CPP framför var någonstans det har skett ett dataintrång, det vill säga varifrån kortuppgifterna som de kriminella använder härstammar ifrån. När man har säkerställt CPP så kan man ta reda på de kortnummer som möjligtvis kan vara kompromet terade. Detta förstärker även det som framkommit i teoridelen av arbetet.

I intervjuerna framkom det även att tredje parter som Visa och Mastercard har en viktig roll i kedjan eftersom de erbjuder informationen om kompromet terade kortnummer till banken.

I intervjuerna framkom det att det förebyggande arbetet kan utföras antingen manuellt eller med hjälp av datorsystem. Respondenterna i intervjuerna föredrar att utföra arbetet manuellt eftersom resultatet enligt deras åsikt och erfarenhet kan bli bättre. Eftersom arbetet handlar om att analysera samt tolka data, och slutresultatet till än hög grad beror på det, kan man konstatera att personer som utför arbetet måste ha en hög analytisk förmåga.

Banker använder i dagens läge maskininlärning främst i det förhindrande arbetet av CNP-kortbedrägerier. Maskininlärning kan även användas i det förebyggande arbetet, men som tidigare sagt, anser respondenterna att slutprodukten ofta är bättre ifall man genomför processen manuellt. Detta tyder till att det i framtiden lönar sig att satsa på att förbättra programmeringen av datorprogrammen för att även automatisera den delen av arbetet till den grad det är möjligt.

Vare sig det handlar om att sätta stopp på eller förebygga CNP-kortbedrägerier så är det viktigt att banken alltid byter ut kortinnehavarens kompromet terade kort för att säkerställa att kortet inte kan användas i bedrägligt syfte i framtiden. Vid samma tillfälle kontaktar banken kortinnehavaren för att berätta om processen som kommer att ta plats. Vilka kommunikationskanaler som används beror på banken och dess interna processer. Generellt kan man säga kommunikationen sker via ett telefonsamtal, textmeddelande, nätbanks meddelande eller per brev.

6 DISKUSSION

Detta examensarbetes syfte är att presentera vad bankerna kan göra för att bekämpa bedrägliga CNP-betalkortstransaktioner samt försök till dessa. Studiens resultat kan som tidigare sagt, anses vara reliabla vid denna tidpunkt, men kan senare påverkas av nya verktyg och nya processer som integreras i verksamheten.

Reliabiliteten på informationen som fåtts i intervjuerna anser jag vara på en relativt hög nivå eftersom jag intervjuat personer som länge arbetat inom ämnet som studerats i finansbranschen. Jag säger relativt hög, eftersom de personerna som intervjuats kommenterade och svarade på frågorna som ställdes i intervjun mera generellt och inte specifikt. Detta eftersom de inte kan avslöja allt som görs på branschen på grund av banksekretesslagen.

Studien visar att den kunskap och de verktyg som i dagens läge finns tillgängliga för banker, även används för att förbättra deras processer. Det enda tydliga stället jag kan tänka mig att banker har råd att förbättra sig i är maskininlärningen i det förebyggande arbetet av CNP-kortbedrägerier. Detta eftersom datorer inte gör mänskliga fel då programmeringen är gjord korrekt och för att datorer generellt gör jobbet snabbare än människor. Eftersom banker vill förebygga kortbedrägerier, kan man anse att ju snabbare arbetet görs, destu mindre tid har kortbedrägarna på sig att använda de komprometterade kortuppgifterna.

Studien lyckades i min åsikt allt som allt bra, eftersom den lyfter fram de centralaste och viktigaste metoderna samt processerna som banker kan använda för att motarbeta CNP-kortbedrägerier. Vissa steg och processer som framkom i intervjuerna skulle jag ha önskat att beröra lite mera detaljerat, men det var inte möjligt eftersom banker har både sekretess samt tystnadsplikt. Därför nöjde jag mig att behandla ämnet mera generellt utan att vare sig jag eller respondenterna tar närmare ställning till något visst företag eller bank och deras processer.

Jag valde att utföra studien med hjälp av kvalitativa semistrukturerade intervjuer. Metoden jag valt för arbetet fungerade bra, eftersom jag kunde diskutera med respondenterna

och ställa följdfrågor till dem. Respondenterna kunde även fritt berätta om sina egna tankar och synpunkter.

Min egen erfarenhet, samt det jag lärt mig om ämnet i teoridelen av arbetet, hjälpte mig i studien eftersom jag, för det första, kunde få tag på rätt personer i tanke på intervjuerna och för det andra, hade kunskapen att ställa de rätta följdfrågorna i intervjuerna.

Jag utförde sammanlagt tre intervjuer med personer som arbetat i finansbranschen under en längre tidsperiod. Respondenternas kunskap, erfarenhet och tillhörande uppfattningar om själva branschen, produkterna och processerna inom ämnet var på en väldigt hög nivå vilket resulterade i djupa intervjuer om ämnet.

Jag anser att antalet respondenter var på en bra nivå för denna studie, eftersom jag fick tillräckligt mycket, samt omfattande svar och åsikter till de frågor jag ställde respondenterna. Jag tror inte att ett högre antal respondenter skulle ha påverkat arbetet dramatiskt, men däremot tror jag att jag kunde ha missat en del kritisk information ifall jag bara utfört intervjuer med en, eller två respondenter.

Tidigare forskning inom ämnet var väldigt begränsat och de studierna jag lyckades få tag på fokuserade sig på att förklara vad CNP-kortbedrägerier är och hur dessa utförs. Valet att undersöka hur banker kan motarbeta CNP-kortbedrägerier gjordes dels på grund av detta, men även dels för att ämnet är väldigt aktuellt i dagens samhälle.

För att inte studien skulle bli för bred, hamnade jag avgränsa studien och valde då att utföra studien ur bankens synvinkel. Ämnet kunde dock även undersökas ur företags och näringsidkares synvinkel, eftersom dessa också har en betydlig roll i kedjan. Ämnet kunde även studeras med fokus på vilka verktyg banker möjligtvis kunde använda sig av för att motarbeta CNP-kortbedrägerier i framtiden.

KÄLLOR

Litteratur:

Brenner, S. W., Project Muse & Copes, H. -. V. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes,* Northeastern University Press, 8–13 s.

Bryman, A. (2012). *Social Research Methods*, 4th edn. Oxford, Oxford University Press, 160 s, 179 s, 330 s, 380 s, 405 s, 470 s.

Christensen, L., Engdahl, N., Grääs, C. & Haglund L. (2001). *Marknads- undersökningen handbok*, 2 upplagan, Studentlitteratur, 164–165 s.

Davies, M. B., & Hughes, N. (2014). *Doing a successful research project, Using qualitative and quantitative methods,* New York: Palgrave, 8–9 s, 23–24 s.

Montague, D. (2010). *Essentials of Online payment Security and Fraud Prevention*, 1st ed., John Wiley & Sons Inc., Hoboken, x s, 38–39 s, 57–59 s, 61–64 s, 111 s, 122 s, 199–200 s.

Wells, J. (2010). *Internet Fraud Casebook: The World Wide Web of Deceit*, 1st ed., John Wiley & Sons Inc., Hoboken, xvii s.

Elektroniska källor:

Albrecht, C., Albrecht, C. & Tzafrir, S., 2011. *How to protect and minimize consumer risk to identity theft,* Journal of Financial Crime, Vol. 18 No. 4, pp., 406–409 s. Tillgänglig: https://doi-org.ezproxy.arcada.fi:2443/10.1108/13590791111173722 Hämtad 28.4.2021

Bergfors, M. (2019). *Polisen vill upplysa om bedrägerier: ”Skammen är bedragarens bästa vapen”,* Svenska.yle.fi. Tillgänglig: https://svenska.yle.fi/artikel/2019/12/23/polisen-vill-upplysa-om-bedragerier-skammen-ar-bedragarens-basta-vapen Hämtad 24.4.2021

Brex.com. (2021). *What is credit card fraud?*. Tillgänglig: https://www.brex.com/learn/fraud-security/what-is-credit-card-fraud/ Hämtad 23.4.2021

Bristow, C. (2021). *What is Transaction Monitoring in AML?*, Sas.com. Tillgänglig: https://www.sas.com/en_ie/insights/articles/risk-fraud/what-is-transaction-monitoring-in-aml.html Hämtad 25.11.2021

Capgemini (2012). *Credit Card Transaction Fraud and Mitigation Trends*, 7 s, 12 s. Tillgänglig: https://www.capgemini.com/wp-

con-
tent/uploads/2017/07/Credit_Card_Transaction_Fraud_and_Mitigation_Trends.pdf Hämtad 27.4.2021

Cassell, C., Cunliffe, A. & Grandy, G. (2017) *The SAGE Handbook of Qualitative Business and Management Research Methods,* 1st edn., SAGE Publications, Kapitel 39. Tillgänglig: https://www.perlego.com/book/860009/the-sage-handbook-of-qualitative-business-and-management-research-methods-pdf Hämtad 26.10.2021

Chen, J. (2020). *Carding*. Tillgänglig: https://www.investopedia.com/terms/c/carding.asp Hämtad 24.2.2021

Daly, L. (2020). *How Do Criminals Steal Your Credit Card Information*?. The Motley Fool. Tillgänglig: https://www.fool.com/the-ascent/credit-cards/articles/how-do-criminals-steal-your-credit-card-information/ Hämtad 23.5.2021

Dwyer, B. (2020). *Credit Card Processing: How it Works,* CardFellow. Tillgänglig: https://www.cardfellow.com/blog/how-credit-card-processing-works/ Hämtad 9.4.2021

European Central Bank (2014). *Card payments in Europe,* 15 s. Tillgänglig: https://www.ecb.europa.eu/pub/pdf/other/cardpaymineu_renfoconsepaforcards201404en.pdf?cca00bd3ff6ef67458ef0d94a1d52518 Hämtad 27.4.2021

Finlex 24.8.1990/769. *Strafflag,* 36 kap. 1 §. Tillgänglig: https://finlex.fi/sv/laki/ajantasa/1889/18890039001#mvs Hämtad 10.4.2021

Fraudpractice.com (2020). *Hot Lists, Warm Lists and Positive Lists*, Fraudpractice.com. Tillgänglig: http://fraudpractice.com/gl-lists.html Hämtad 25.11.2021

Galletta, A. (2013) *Mastering the Semi-Structured Interview and Beyond*, NYU Press, Kapitel 12. Tillgänglig: https://www.perlego.com/book/719356/mastering-the-semistructured-interview-and-beyond-pdf Hämtad 26.10.2021

Gottschalk, P. (2010). *Policing Cyber Crime*, 10 s. Tillgänglig: https://1library.net/document/ozlo26rz-policing-cyber-crime-pdf.html Hämtad 26.10.2021

Holmes, I. (2021). *How to uncover common point of purchase*, Sas.com. Tillgänglig: https://www.sas.com/en_us/insights/articles/risk-fraud/common-point-of-purchase.html Hämtad 25.11.2021

Nordea Bank Oyj. (2021). *Pankki- vai luotto - debit vai credit?*. Tillgänglig: https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/credit-vai-debit.html Hämtad 10.5.2021

Polismyndigheten (2019). *Kostnaden för bedrägeribrott med kortuppgifter: Två miljarder*. Tillgänglig: https://polisen.se/aktuellt/nyheter/2019/november/samlat-grepp-behovs-for-att-komma-at-kortbedragerierna/ Hämtad 24.2.2021

Puurunen, T. (2018). *Poliisi kehottaa tarkkailemaan tilitapahtumia: tietomurroilla varastettuja luottokorttitietoja voidaan käyttää vuottakin myöhemmin*, Yle.fi. Tillgänglig: https://yle.fi/uutiset/3-10485287 Hämtad 24.2.2021

Vuorimäki, T. (2020). *Maksuvälinepetoksia on tehty viime viikkoina tavallista enemmän – Rypäs viittaa tietomurtoon,* Aamulehti.fi. Tillgänglig: https://www.aamulehti.fi/uutiset/art-2000007426865.html Hämtad 24.2.2021

BILAGOR

Bilaga 1: Intervjuguide

Bakgrundsfrågor om CNP-kortbedrägerier

1. Vad är kortbedrägeri för något?

2. Vad anser du vara skillnaden mellan kortbedrägeri och CNP-kortbedrägeri?

3. Hur vanliga är CNP-kortbedrägeri i dagens samhälle?

4. Kommer antalet CNP-kortbedrägeri växa i framtiden?

5. Varifrån får de kriminella tag på kortuppgifterna som behövs för att utföra CNP-kortbedrägerier?

6. Vems arbetsuppgift är det att förhindra och förebygga CNP-kortbedrägeri?

Förhindrande arbete av CNP-kortbedrägerier

7. Vad handlar det förhindrande arbetet av CNP-kortbedrägeri om och hur skulle du definiera arbetet?

8. Hurdana processer kan banker använda för att hitta de bedrägliga korttransaktionerna? (Robotar? Maskininlärning? Datorsystem?)

9. Hurdana processer har banken när det gäller hanteringen av de bedrägliga transaktionerna?

10. Hurdana tecken letar banken efter när det gäller att hitta CNP-kortbedrägerier?

11. Använder banker så kallade heta listor?

12. Hurdana processer har banken när man misstänker att en transaktion är bedräglig?

13. Hur säkerställer banken att det inte görs fler bedrägliga korttransaktioner med kortet?

14. Vad händer ifall det visar sig att transaktioner är gjord av kortinnehavaren själv/inte gjord av kortinnehavaren själv?

15. Hur sköts kontakten/vilka kommunikationskanaler använder banken för att kontakta kortinnehavaren?

Förebyggande arbete av CNP-kortbedrägerier

16. Vad handlar det förebyggande arbetet av CNP-kortbedrägeri om och hur skulle du definiera arbetet?

17. Hurdan data använder banker för att kunna förebygga CNP-kortbedrägerier?

18. Varifrån fås den data som behövs för att kunna förebygga CNP-kortbedrägerier?

19. Handlar det förebyggande arbetet av CNP-kortbedrägerier om manuellt arbete eller använder sig banker av andra metoder? (Robotar? Maskininlärning? Datorsystem?)

20. Vad är en CPP?

21. Hur förhindrar banken CNP-kortbedrägerier efter att man har fått veta att kortnumret är kompromitteret?

22. Kontaktas kortinnehavaren i något skede av processen?

23. I vilket skede och via hurdana kommunikationskanaler?

24. Är det något du vill kommentera eller lägga till?

Tack för intervjun.