Haaga-Helia
University of Applied Sciences

A look into CNP Fraud and its prevention

Olga Sergunina

Bachelor's Thesis
Degree Programme in
International Business
2017

Table of contents

Author(s)
Olga Sergunina

Degree programme
International Business

Report/thesis title	**Number of pages**
A look into CNP Fraud and its prevention	64

The thesis is a look into payment card fraud in Finland and Europe. The focus is especially on card-not-present (CNP) frauds, which occur in scenarios when merchants are processing payments on e-commerce websites, where payment card is not physically present.

The goal of the thesis is to provide a comprehensive insight into card fraud and learn about its prevention services that are provided by banks to cardholders.

To understand the topic, the theory part includes a desktop study. It includes the following subjects: basics of payment card industry, financial and internet crime, CNP fraud process and techniques. Additionally, the study presents statistics on card fraud in Europe and in Finland to understand the scope of card fraud in the area and see the trends. When the basic topics are studied, the thesis discusses technologies that are available in the industry to prevent card fraud. The theoretical study uses reliable secondary data sources such as theoretical works, reports from the card and card fraud prevention industry found on trustworthy webpages.

The research part of the thesis investigates card fraud prevention services that are available in three selected leading banks, which operate in the territory of Finland: OP bank, Nordea bank and Danske bank. The data is collected from the official websites of the selected banks and reviewed. Furthermore, card fraud prevention services are analysed and compared to fraud mitigation methods that have been studied in the theoretical framework. As a result, the research provides a thorough review of card fraud prevention services and suggests the analysed banks to adopt or develop certain services to improve security of cardholders' assets.

Keywords
card fraud, CNP, identity theft, online payment fraud, card fraud prevention, identity authentication

1 Introduction

1.1 Background

Payment card fraud is a hot topic in the financial crime area. It is a highly profitable criminal activity and it involves minimal risk for the organised criminal groups, who control the entire European criminal market of card fraud. The issue is on a global scale and losses due to card fraud are increasing from year to year. (Europol 2012, 3.) Thus, it is very important for all parties, including banks and cardholders to be aware of current card fraud methods and be able to implement and use appropriate security measures.

Last year I have become a victim of a debit card fraud myself. Three unauthorized transactions have occurred on a Visa electron card, which was issued by an OP Financial Group. The fraudulent payments have been discovered when using internet banking to pay monthly bills. The card was not physically stolen, but the card data has been compromised and it is not known how the fraudsters have obtained the information. The transactions have taken place on e-commerce websites in India and were very untypical for my spending habits. This experience gave me an inspiration to write this study and learn how the card data could have been stolen and how I could have prevented it with the help of my bank.

1.2 Research Question

The objective of the thesis is to understand how unauthorised transactions occur when a payment card is not physically stolen and what services provided by banks help to prevent them. The research question can be worded as “How do banks prevent card fraud?” In order to conduct the research the RQ is divided into investigative questions (IQ):

IQ 1. “What card fraud prevention services do banks provide?”
IQ 2. “How can banks develop fraud mitigation services?”

The theoretical part of the thesis will first study basics of the payment card industry and financial crime as an introduction to the topic. Then the most common card fraud methods and card fraud prevention techniques available in the industry will be examined. Additionally, the study will look at card fraud in Europe and particularly in Finland to understand the scope of the problem in the area. The main task of the theory part is to provide a comprehensive insight into card fraud and its prevention. Further it will allow to perform a research on the topic. In the theoretical study, reliable secondary data sources such as books, peer reviewed articles and reports from the card and card fraud prevention industry found on trustworthy webpages were used.

The research part will investigate card fraud prevention services provided by Finnish and Nordic leading banks. For that purpose, three case banks have been selected: OP bank, Nordea bank and Danske bank. Data for the research has been collected directly from official webpages of the selected banks and used for comparison and evaluation. The study will compare the existing fraud mitigation services with the theoretical material studied and based on that will suggest banks new fraud mitigation techniques to adopt. As a result, the research will provide a broad overview of the existing card fraud prevention services in the case banks and identify points for improvement. This will allow to answer IQ 1 and IQ 2.

Table 1 below presents theoretical framework, research methods and results chapters for each investigative question.

Table 1. Overlay matrix

Investigative question	Theoretical Framework	Research Methods	Results
IQ 1. "What card fraud prevention services do banks provide?"	**2.4.** CNP payment process **3.4.** CNP Fraud **5.** Card Fraud Prevention	-Secondary data research	**7.** Banks' services for card fraud prevention
IQ 2. "How can banks develop fraud mitigation services?"	**4.** CNP fraud in EU and Finland **5.** Card Fraud Prevention	- Comparative analysis	**8**. Results

1.3 International Aspect

Payment card frauds in Europe are large-scale crimes with international dimension. European Union is very vulnerable to unauthorised transactions done overseas: victims that are located within the EU zone are commonly targeted by fraudsters outside of EU especially when the use of internet is involved. (Europol 2012, 3.) The cross-border unauthorised transactions bring the problem of card fraud on international level. The unauthorised transactions mentioned in the introduction have also taken place outside of Europe – on Indian e-commerce websites, while the cardholder was located in Finland.

Another international aspect of the research is comparative analysis, which will involve one local Finnish bank and two international banks. Security services for preventing unauthorized transactions in the banks will be compared and evaluated. It will allow to see how the problem of card fraud is being addressed by different banks, which have different geographical coverage.

1.4 Benefits

The thesis is intended to provide up-to-date information on payment card fraud to spread awareness among cardholders about the current fraud techniques, because unfortunately not that many people are educated about security of their payment cards. Further the research part will inform about the existing card fraud preventative services provided by banks nowadays. When cardholders are aware of the options available to protect their payment cards and funds they will be able to find the suitable financial institution, which offers needed card fraud preventive services for them. Furthermore, the benchmarking done between banks in the research part will demonstrate card fraud preventative services, which the banks are still lacking and which they could implement in order to provide more security services to their clients.

I also see this thesis to be of a great value to myself, because I have learnt a lot about payment card industry. The knowledge of card payment process and payment card fraud that I have gained is of benefit in my career, because my profession is closely related to payment administration in online business and I am working with payment service providers on daily basis. Dealing with card fraud and chargebacks is a part of online business.

1.5 Key Concepts

Cardholder – is a person or organisation, who has obtained a payment card from card issuing financial institution (bank) and is a rightful owner of the payment card (European Central Bank 2014, 17).

Card-not-present (CNP) transaction – is a type of payment transaction, which occurs in a scenario when a merchant is processing payment without card being physically present (Laudon & Traver 2017, 294). Focus in this paper is on CNP transactions that taken place on e-commerce websites.

Payment Card Fraud – is a misuse of prior stolen payment card details by initiating payments, fund transfers and cash withdrawals under cardholder's name (Gottschalk 2010a, 445).

Identity Theft – is a crime, which involves theft of valuable personal or financial information, which further could be unlawfully used for impersonating the owner and gaining financial benefits. Examples of the personal data are: social security number, passport details, driver's license number, payment card details. (Gottschalk 2010a, 450.)

Identity authentication – is a process of checking identity of a person, who is initiating a payment transaction and ensuring that this person is a rightful cardholder of the card used for making the payment transaction in question (EMV Migration Forum 2016, 7).

2 Card payment industry

In order to study card payment fraud and its prevention it is important to understand the basics of the card payment industry first. This chapter will briefly study the following topics: types of payment cards, types of payment transactions and the payment process itself.

2.1 Payment cards

There is a number of various payment cards types all over the world, but the subchapter will be discussing the ones that are in use in the Eurosystem. They are presented in the Figure 1. The types of payment cards are typically distinguished by point of time when a payment is debited to the user's bank account (European Central Bank 2014, 15).

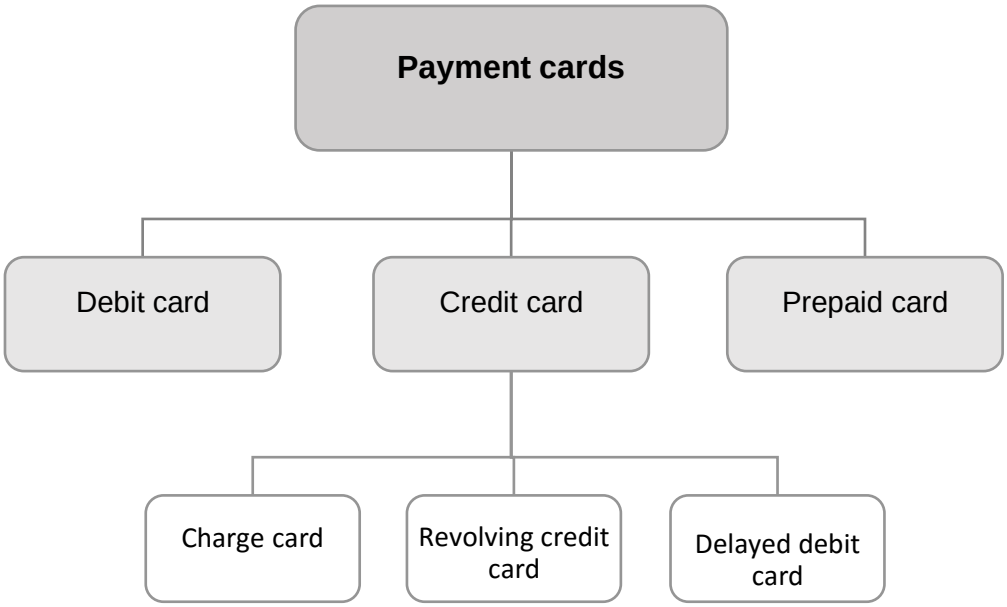

Figure 1. Payment card types

For example, with the use of debit card funds are debited straight from the customer's bank account automatically at the moment of payment transaction. European Central Bank (ECB) refers to this type of payment as "pay now" model. Spending limit on a debit card will be equal to the total amount of funds available on the cardholder's bank account. (European Central Bank 2014, 15.)

Credit card on the other hand allows customer to make purchases and withdraw cash within the credit limit, predetermined by a financial institution – credit provider. The credit cards operate based on a "pay after" model. Credit settlement happens in the end of specified

time period (for example in the end of each month). There are also subtypes of credit cards. For example, when credit has to be paid in full by the end of the specified period, then this type of credit card is called charge card. Credit can also be settled in part, however in that case interest is added to the credit balance. ECB classifies this type of credit card as revolving credit card. (European Central Bank 2014, 15.)

Due to the fact that with the credit card customer is not charged directly at the moment of purchase, the credit card schemes' regulations and transaction processing are broader than debit cards'. Thus, ownership of a credit card gives vast opportunities to make payments in more card acceptance scenarios, than ownership of a debit card. Depending on a type of credit card's scheme different style of card will be granted. Typically, there are the following two categories differentiated: basic and exclusive (for example: platinum, golden, etc.) (European Central Bank 2014, 15.)

Delayed (deferred) debit card is a variation of a credit card without granted credit. The delayed debit card allows customer to make purchases and withdraw cash from ATM machines within a limit, which is authorized by a financial institution of the cardholder. The payments are charged to customer's bank account, but will be fully settled in the end of specified time period. (European Central Bank 2014, 15.)

There are also exist prepaid cards, which work by "pay before" model. A cardholder loads balance on a prepaid card beforehand to be able to make purchases later. However, prepaid card is not the same as electronic purse, which holds electronic money on a chip of a card or on a server. According to Eurosystem policy electronic purses are classified as e-money, but not as a payment cards nor as payment transactions. (European Central Bank 2014, 15.) Thus, electronic purses are not applicable to the current research.

Payment cards are issued by local banks and financial institutions. Cards can also be classified as consumer and commercial types. Consumer cards are the cards that are issued by financial institutions to private individuals for personal use. Opposite to consumer cards, commercial cards are made for the use of a company and its employees, as well as for the use of individual entrepreneurs, in business purposes. Users of commercial cards are usually charged higher fees by banks. (European Central Bank 2014, 15.)

In this sub-chapter, it can be noted that credit cards would be the most attractive target for fraudsters since credit card potentially allows to misuse more funds than a debit card, which is limited to the funds only available on a bank account. Additionally, cardholder makes a settlement of the credit card bill only in the end of a specified period, which

2.2 Card payment transactions

Card payment transactions in payment card industry are divided in two different types: Card-Present (CP) and Card-Not-Present (CNP) as demonstrated in Figure 2. The type is determined by physical presence of a card during payment transaction. (Montague 2010, 10.)

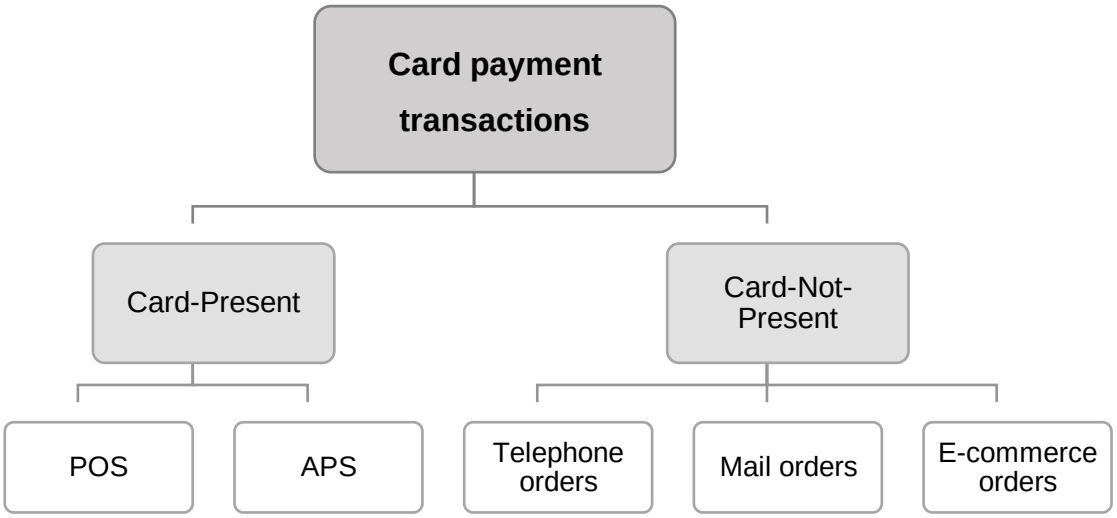

Figure 2. Types of card payment transactions (Montague 2010, 10; European Central Bank 2014,16)

CP transaction can occur at a physical point of sale (POS), where consumer purchases goods or services by physically handing a payment card to a merchant, who in turn processes the order (for example purchase in a shop). Another scenario for CP transaction is a payment at attended point of sale (APS). APS can be a vending machine, a machine for parking payments and such, where a merchant is not present during the actual payment process, but a payment card was still physically used. This type of CP transactions usually has very low value payments. (European Central Bank 2014, 16.)

CNP transactions on the other hand are the transactions that happen remotely, when a merchant (or a machine) does not physically hold or see consumer's card to process a payment. For that reason, CNP transactions are the most vulnerable for fraud and lead to the biggest amount of chargebacks. (Laudon & Traver 2017, 294.)

CNP has three sub-groups: 1) telephone orders or so called phone-in-orders (orders placed and processed on a phone), 2) mail orders or so called catalogue orders (sending an order in a letter by mail) and 3) e-commerce orders (online shopping). (Montague 2010, 10.) The focus of this study will be on CNP transactions, which occur in e-commerce environment.

2.3 E-commerce payment types

E-commerce payment transactions can occur in different scenarios and between different parties. The e-commerce types have been defined according to the market relationship (Laudon & Traver 2017, 56). The sub-chapter will briefly discuss them to identify the e-commerce payment type that is applicable to the research.

The first type is B2B e-commerce. It is a business-to-business selling model through online platforms (Laudon & Traver 2017, 58). In this scenario one of the companies is in a position of a buyer and another company is a seller - online business, which is offering products or services for purchase. Payment transactions occur between businesses only. (Radu 2003, 1.) It is the biggest type of e-commerce that accounts for volume of € 14.2 trillion in transactions all over the world (Laudon & Traver 2017, 58). A good example of B2B e-commerce payment is organization's purchases of raw materials from a supplier. Sometimes B2B payments take place within the same organization. It can happen, for example, when one of the departments is producing goods and another is purchasing them.

B2C e-commerce has business-to-consumer selling model, where online business targets consumers, not companies, to make a sale. In B2C selling buyer is an individual customer, who is purchasing goods or services from a seller – online merchant. Examples of B2C e-commerce purchases are: retail goods, travel services, and online content. It is worth to mention that this type of e-commerce has grown significantly since 1995 and continues to expand. (Laudon & Traver 2017, 57.)

And the last is C2C e-commerce type, which is a consumer-to-consumer selling model, where individuals are able to trade directly with other individuals with a use of the Internet platforms. It is has become possible by utilizing an online market makers, so-called platform providers. In other sources this model is referred as (P2P) person-to-person (Radu 2003, 1).

The study will be primary discussing B2C payment transactions in e-commerce environment, specifically the payments for retail goods by consumers in Finland and Europe. Thus, size of B2C e-commerce and its growth in Europe will be studied later in the paper.

2.4 CNP payment process

Card payment transaction process description vary from source to source. Thus, I have analysed several publications provided by European Central Bank, by major card networks Visa and MasterCard and by the independent source for original CNP news – CardNotPresent.com. As a result, I have unified the descriptions from the above-mentioned sources providing a clear depicting of the CNP payment transaction.

2.4.1 Main actors

Before moving to analysing the card payment process it is essential to determine the key actors that are involved in the process. The central actor is a cardholder, who is a payer in the payment scenario. A cardholder could be an individual or a company, who is an authorized user of a payment card. The payee on the other hand is called card payment acceptor - an individual or a company, who is an authorized card acceptor. (Visa 2013, 9.)

Among other actors in the payment process is a card issuer (issuing bank). It is a financial institution, typically, but not always, a bank, which issues payment cards. A cardholder obtains a contract and a payment card from an issuer. Card payment acceptor also enters into a contract with a financial institution. This Financial institution is called card acquirer. (European Central Bank 2014, 17.) An acquirer is responsible for accepting and processing card payments. An acquirer is also can be called “merchant bank”. (Visa 2013, 9.)

For the technical processing in the card payment operation processing entities are responsible. There are two processing entities on both sides: issuing processor and acquiring processor. Issuing processor does opening and managing of cardholder’s account as well as booking and authorization of their payment transactions on behalf of card issuer. Additionally, issuing processor can perform clearing and settlement. That would include handling chargebacks as well. An acquiring processor on the other hand manages card payment acceptor’s account on behalf of a card acquirer, sends authorization requests to issuing processor, records payment transactions to card payment acceptor’s account and charges fees for the service. (European Central Bank 2014, 17-18.)

An Intermedium for all these actors is a card network. It basically links issuing and acquiring entities and facilitates a payment flow between them. There are the following major card networks on the market: Visa, MasterCard, Discover and American Express. (Credit Card Insider 2017.) Lastly, clearing house is an entity that is involved in clearing and settlement processes between card issuer and card acquirer. Through clearing house transfer

instructions for funds, securities or other instruments are being exchanged. (European Central Bank 2014, 18.)

2.4.2 Authorization

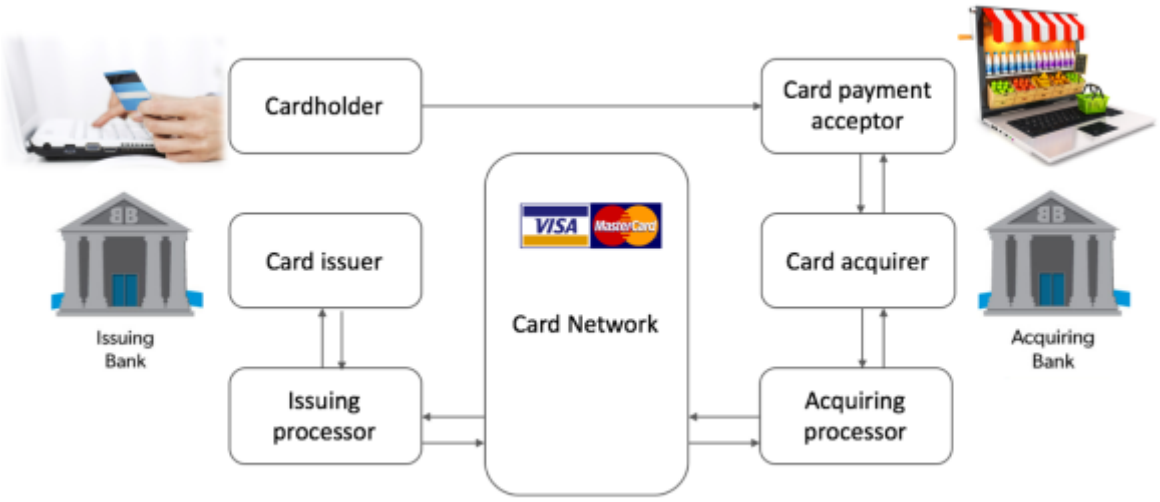

Figure 3. Authorization process. (Visa 2013, 10; MasterCard 2007)

Authorization process is the initial step in the payment transaction. During authorization process it is verified if the payment card used is valid and the payment funds are being reserved. When cardholder enters card's information on the merchant's website and proceeds to the purchase, card acquirer (merchant bank) receives the card information. Card acquirer will route the information through the acquiring processor to the card network that connects the card acquirer and the card issuer. Card network will check security details on the card and identify to which issuing bank (card issuer) does the certain payment card belong. Further the request for purchase approval is being directed through issuing processor to card issuer, which in turn will verify that the card was issued to the particular buyer. If it is a credit card then credit limit will be checked and in case of debit card - cardholder's balance available on the moment of purchase. Once the issuer approves or rejects the transaction the answer is sent back to the processor, which forwards it to acquirer and finally to card payment acceptor to complete the purchase. (Visa 2013, 10; MasterCard 2007; Card Not Present 2015.) The whole process takes a few seconds on average, but has a lot of importance for fraud prevention, because during this phase identity authentication of a cardholder takes place.

2.4.3 Identity authentication

For CNP transactions strong identity authentication of a cardholder during payment authorisation process is vital, because the payer is not physically present at POS. Thus, the identity of cardholder has to be prooved in order to prevent potential online payment fraud. Identity authentication process can rely on three authentication factors:

1) Ownership factor – something that cardholder has (credit card, mobile device)
2) Knowledge factor – something that cardholder knows (PIN code)
3) Inherence factor – something that cardholder is (fingerprint, facial features)

Authorising payment based only on one authentication factor will involve high risk. Usually it is recommended to incorporate all three factors or at least two. Such authentication with multiple layers is called multifactor and provides more confidence that the transaction is not frauddulent. (EMV Migration Forum 2016, 7.)

2.4.4 Clearing

Typically, within on day after authorization has been completed process of clearing will take place. It starts by card acquirer (merchant's bank) sending purchase details to card network through acquiring processor. Clearing house of the given card network will be validating the information provided and directing it to the card issuer (cardholder's bank) through issuing processor. The issuer in turn will prepare cardholder's statement. Clearing process is completed by clearing house performing comprehensive reconciliation of the payment and providing the results to the acquirer and the issuer. (MasterCard 2007; European Central Bank 2014, 18.)

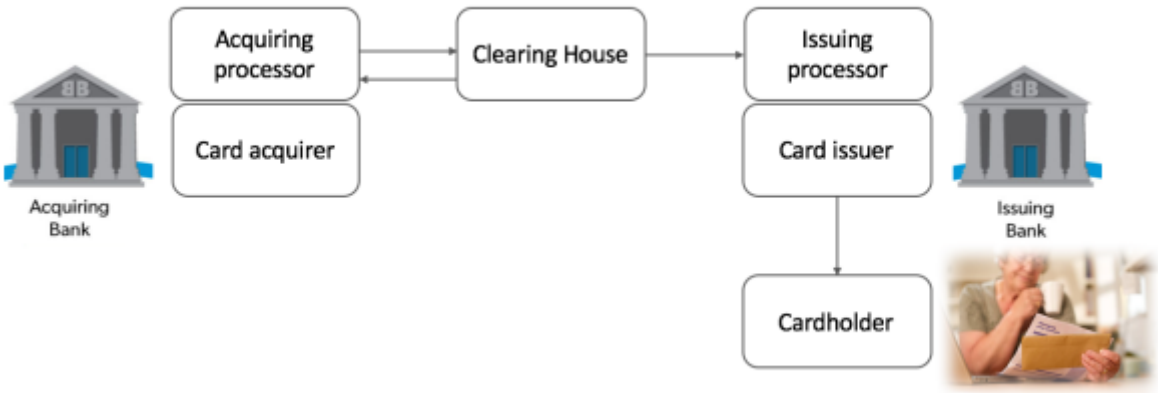

Figure 4. Clearing process (MasterCard 2007)

2.4.5 Settlement

At this point the payment funds were only “captured”, reserved on the cardholder’s account, but the card issuer has not sent the actual payment to the card payment acceptor yet. For that to happen the merchant has to initiate a process of settlement. He will usually do it in the end of the day or specific time period or after the goods have been shipped to the buyer. Settlement is being done for a batch of transactions at once and for that reason the process is often called “batching”. Information on the batch of transactions is being submitted to the acquirer and routed through acquiring processor to card network. Card network will be facilitating the payment settlement by sending an order for payment to the issuer. The funds will be transferred to the acquirer on average within 24 hours. (Visa 2013, 14.)

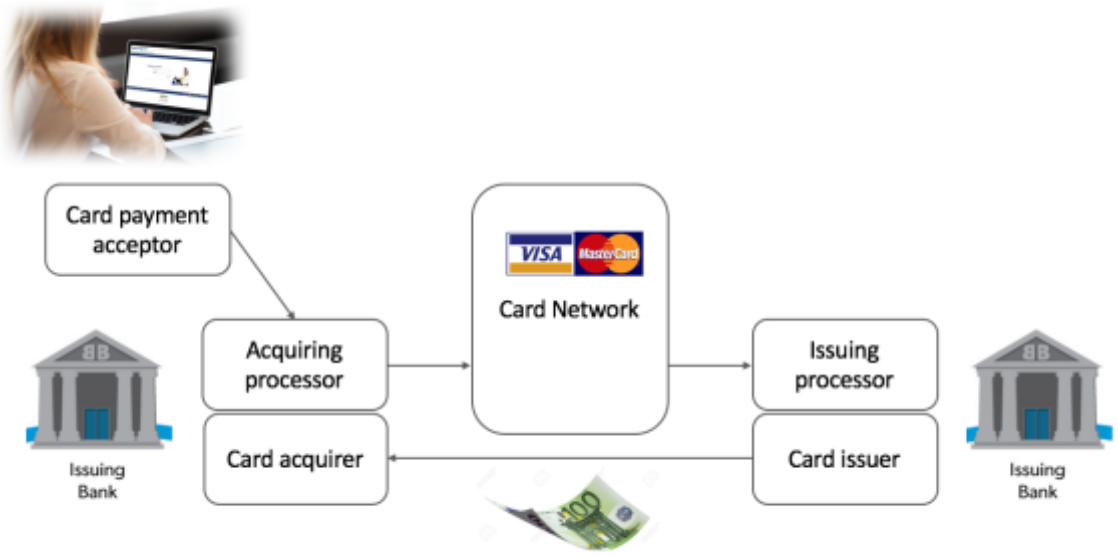

Figure 5. Settlement process (Visa 2013, 14; MasterCard 2007)

3 Criminology

In this chapter Financial and Internet Crimes will be defined and their main categories will be studied as a base of theory framework. It will help to identify which types of financial and internet crimes can be involved into card fraud. Further, will be studied a CNP fraud process itself and the most common techniques of perpetrating CNP fraud.

3.1 Financial Crime

Financial Crime is the fundamental theory for the study. Financial crime can be defined as a profit-driven crime, which involves obtaining access to and control over victim's assets by means of deception (Gottschalk 2010a, 441; Pickett & Pickett 2002, 2). Pickett and Pickett (2002, 2) also refer to financial crime as a white-collar crime and highlight that it is nonviolent in its nature. In comparison, violent crimes such as murders and robberies involve physical assault and can be addressed with direct and quick countermeasures by law enforcement agencies. While financial crimes perceived as nontraumatic, without involvement of physical factor, thus nonviolent. Furthermore, the authors identify six components of financial crime as demonstrated in Figure 6. (Pickett & Pickett 2002, 2.)

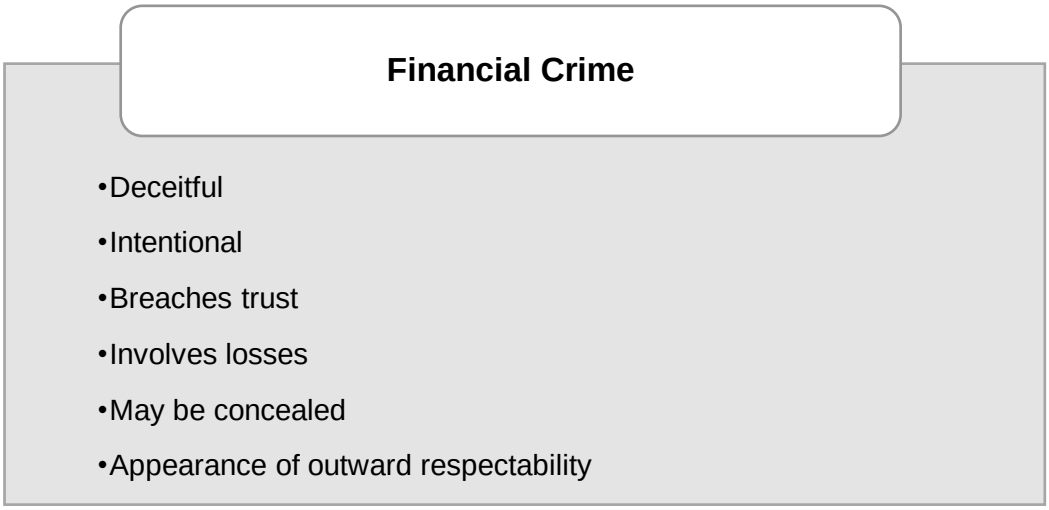

Figure 6. Components of financial crime. (Pickett & Pickett 2002, 2)

The first and main feature of financial crime is deceitfulness. People, who are perpetrating financial crimes, act under false pretences. Gaining victim's financial resources by means of deception is the distinguishing feature of financial crime. Second component is intention of the crime. It is a very important characteristic, because an accidental mistake is not classified as an illegal deed, but seen as a human error. While intentional, planned in advance actions that involve gaining access to someone else's property result in a crime.

As a third component Pickett and Pickett (2002, 2) name breach of trust. In a situation when one party's financial funds were compromised it is apparent that trust, for example, towards second party will weaken either it is a business, service or financial institution (Pickett & Pickett 2002, 2). Since in this paper financial crime like card fraud will be studied, the breach of trust will appear in relationship between bank and its client, who became victim of a card fraud.

The forth component of states that financial crime will certainly involve financial losses, which afterwards will be written off, insured against or accepted. The fact that financial crime can be and usually is concealed is a fifth characteristic. Some perpetrators continue stealing without being revealed for long periods of time. For example, by forging financial documents, altering payment transactions and concealing it by making transactions look regular. The last feature of financial crime is an appearance of outward respectability. Quite often perpetrator turns out to be a regular college, trusted manager or even more often person from the top of a company. Generally, those felonious people or companies come across as trustworthy and reliable to mislead their victims. (Pickett & Pickett 2002, 2.)

Gottschalk (2016, 5) divides financial crime into four main categories: Fraud, Theft, Manipulation and Corruption (Figure 7).

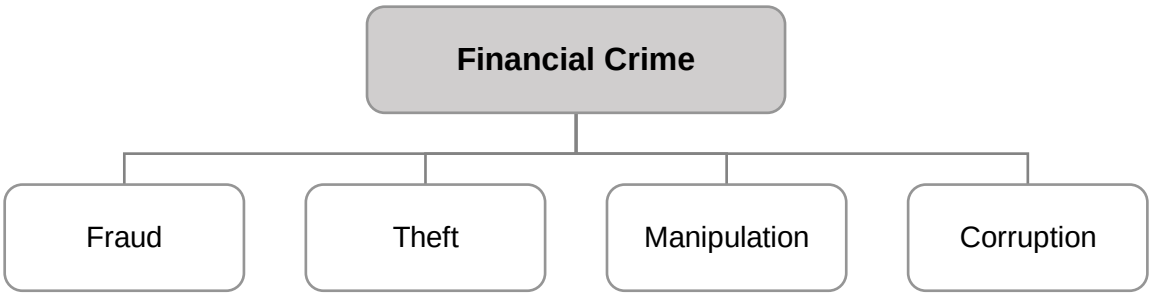

Figure 7. Main categories of Financial Crime (Gottschalk 2016)

In a 4th edition of "Fraud Examination" book by Albrecht, Albrecht, Albrecht & Zimbelman (2011a, 7), the authors define fraud as diverse methods that are used by a human or a group to gain an advantage over another human's or organization's property and assets with a use of false representation. They say that fraud commonly includes: surprise, knavery, trickery, devious and unfair ways to deceive a victim. To make a precise definition the authors have identified 7 crucial components of fraud: 1) A representation 2) about a material point, 3) which is false, 4) and intentionally or recklessly so, 5) which is believed 6)

and acted upon by the victim 7) to the victim's damage. (Albrecht at al. 2011a, 7.) These elements help to understand a definition of fraud and distinguish fraudulent acts from, for example, mistakes.

Fraud itself has various types. Some of the examples are: advance fee fraud, bank fraud, cheque fraud (in countries where such are in use), click fraud, consumer fraud, embezzlement, hedge fund fraud, payment card fraud, mortgage fraud, occupational fraud, subsidy crime, etc (Gottschalk 2016, 5-13.) Card fraud as a subtype of fraud is a primary focus of this paper.

An illegal possessing of one or several individuals' property or any kind of assets without his/her/their permission or authorization is called theft. Theft category can be divided into two sub-categories: tangible and intangible. Tangible sub category includes theft of physical valuable items and assets, for example, theft of cash, inventory, art theft etc. Intangible on the other hand relates to thefts such as intellectual property crime, identity theft. (Gottschalk 2016, 13-16.) Identity theft relates to the research and will be discussed further in the paper.

Manipulation category covers crimes, which involve elements of manipulation such as means of obtaining illegal leverage over activities or results. Examples of manipulation crime are: bankruptcy crime, bid rigging, competition crime, counterfeit currency, ghost employees, income tax crime, inflated invoices, money laundering, etc. (Gottschalk 2016, 16-21).

The last category is corruption. The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) has defined corruption in its Annual Report 2008 as misuse of one's job position for personal advantage. In the same report has been done a reference to the Penal Code, which gives a broader definition of corruption: an offer, request, acceptance or reception of an inappropriate benefit, which relates to a job position, business, or job responsibilities. The inappropriate benefit is not necessarily associated with a certain action or with not-doing that action, but can be linked to a person's job position, business, or job responsibilities. It not only relates to financial gains, but also to pursuing a certain job position or responsibilities. (Økokrim 2008, 15.) Corruption may include: bribery, kickbacks, extortion, etc. (Gottschalk 2010a, 443).

3.2 Internet Crime

Criminal offenses that are perpetrated with the use of and knowledge of computer technology and network are titled as Computer crimes. As well as offenses against a computer and a computer network are Computer crimes or so-called Cybercrimes. An example of computer crime, where computer plays a role of an instrument, is gaining control over corporate's computer system and illegally gaining private information. The perfect illustration of a crime against a computer is an attack on company's computer network and crush of the system. (Laudon & Laudon 2015, 155, 289.) If apart from a computer and its system during the criminal act have been used internet network, then the crime will be already classified as Internet crime (Gottschalk 2010b, 10).

Shipley and Bowker (2014, 2) mention an interesting thought that quite often internet crimes are the new versions of traditional crimes, which were just brought to the internet platform. An example could be an identity theft, which can happen in real life by physically stealing personal ID card, passport or similar. With the development of the internet over the past years it is not necessary anymore to be deft with your hands, but skilful hackers can steal your personal information through the online websites without leaving their home. How it happens will be discussed further in the paper.

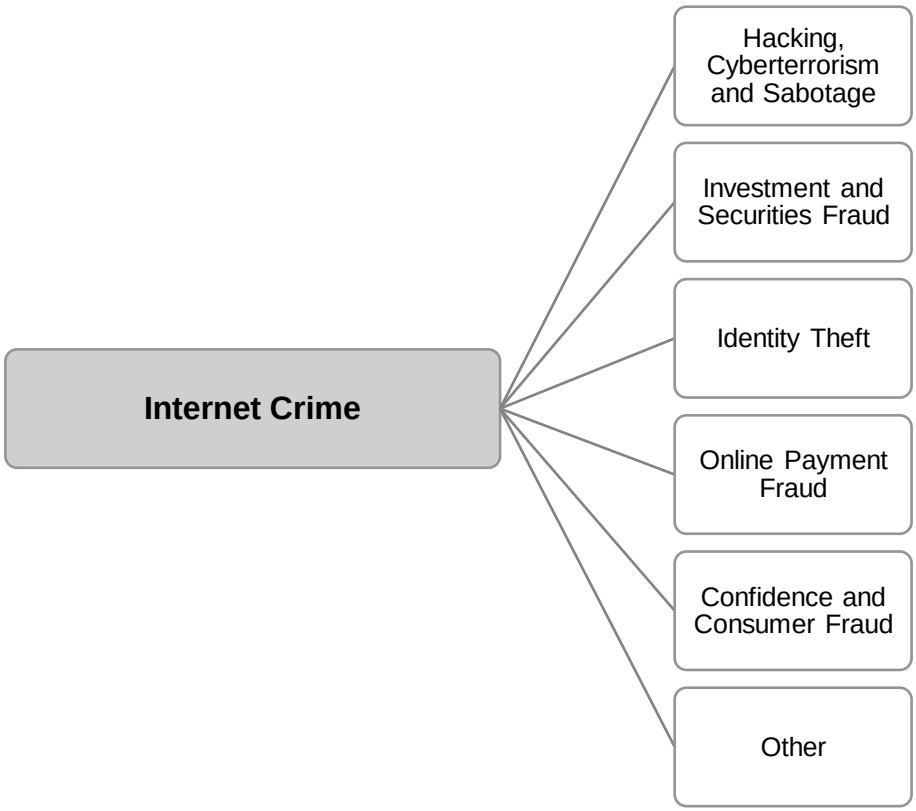

Figure 8. Internet Crime and its subtypes (Wells 2010, xvii)

There are numerous forms of internet crime. Joseph T. Wells in his book “Internet Fraud Casebook: The World Wide Web of Deceit” (2010, xvii) categorizes them into the following groups: Hacking, Cyberterrorism and Sabotage; Investment and Securities Fraud; Identity Theft; Online Payment Fraud; Confidence and Consumer Fraud, etc. (Figure 8)

Hacking, Cyberterrorism and Sabotage category includes crimes like online advertising fraud (pay-per-click manipulation), web site hijacking, online corporate espionage, etc. Such crimes involve use of viruses, malware, keylogging, and other malicious products. (Wells 2010, xvii.) These malicious tools have a very big application in the card fraud activities as well and being used nowadays constantly. The most popular card fraud techniques that utilize hacking will be studied further in this chapter.

Investment and Securities Fraud category involves deceiving a victim into investment scheme and fraudulently manipulating with the funds. Famous examples for these crimes are: Ponzi or pyramid schemes, non-existent investments, misrepresentation of offering and market manipulation. (Wells 2010, xvii.)

Confidence and Consumer Frauds are the crimes that are committed against individuals – consumers. Such frauds are usually perpetrated by fraudulent “companies” in order to deceive the buyer into buying a fraudulent product, involve a victim into a scam and get his money. (Albrecht & al. 2011a, 529-531.) The examples are advance-fee schemes, debt-elimination schemes, charity solicitations, vacation or timeshare solicitations, charges for undelivered services and goods, work-at-home or business opportunities, online auction fraud (Wells 2010, xvii).

Identity Theft category covers all crimes that relate to obtaining victim’s personal, financial or any other valuable details. As a subtype of internet crime, identity theft will imply theft of personal and financial information with a use of internet. Examples of used techniques in this crime are phishing and pharming. (Wells 2010, xvii.)

Online Payment Fraud involves such acts like unauthorised fraudulent online payments, fraudulent check scams, PayPal or Escrow scams, and invalid credit/debit card numbers scam (Wells 2010, xvii). The study will be focusing on the unauthorised online payments as a component of CNP fraud.

It can be concluded that the internet crimes that have a direct relation to the study are: Hacking, Identity Theft and Online Payment Fraud. The elements of these crimes and their role in CNP fraud will be discussed further in this chapter.

3.3 Financial Internet Crime

It is important to understand that Internet Crime is not a category of Financial Crime (Figure 9), but a separate type of crime. Part of financial crimes are perpetrated over the internet, thus will be classified as internet crimes as well. And vice versa. Not all internet crimes are profit-driven and only a part of them will be classified as financial crimes. For example internet sabotage. In the context of this research the focus will be on crimes, which fall into both categories: financial crimes, which are committed with a use of internet. Other intentions than financial gains are excluded. In this paper these types of crimes will be referred as Financial Internet Crime.

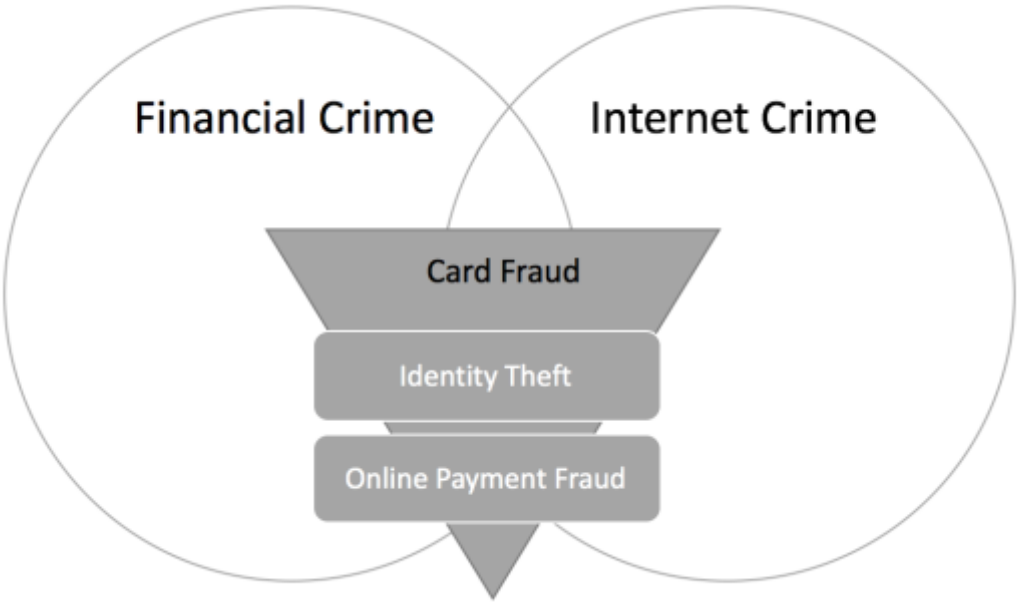

Figure 9. Financial Internet Crime

The crime, which will be investigated in this paper is a CNP fraud, which can be defined as a misuse of prior stolen payment card details by initiating an authorised payment in card-not-present environment (Gottschalk 2010a, 445; Laudon & Traver 2017, 294).

According to the prior studied crime theory, CNP fraud can be divided into two components: 1) identity theft, which precede the second stage 2) online payment fraud. Financial crime classification (Figure 7) identifies the crimes as the fraud and theft (intangible) subtypes. And according to the theory of internet crime the offenses fall into two categories: online payment fraud and identity theft (Figure 8). It means that CNP fraud is a financial crime that can be perpetrated with the use of internet.

3.4 CNP Fraud

CNP fraud is the fraud that has been committed by initiating an unauthorised CNP payment transaction. In the chapter CNP fraud process will be studied as well as how card payment details can be stolen and utilised further in online payment fraud.

3.4.1 CNP Fraud process

In article “How to protect and minimize consumer risk to identity theft” from Journal of Financial Crime authors Albrecht C., Albrecht C., and Tzafrir S. (2011b, 406) describe identity theft process as a cycle. This theory can be applied to Card Fraud process (both CP and CNP frauds), because it involves an identity theft element. Thus, I have taken this theory as a base and described the CNP Fraud process in three stages: 1) Identity Theft (Discovery) 2) Preparation (Action) 3) Online Payment Fraud (Trial).

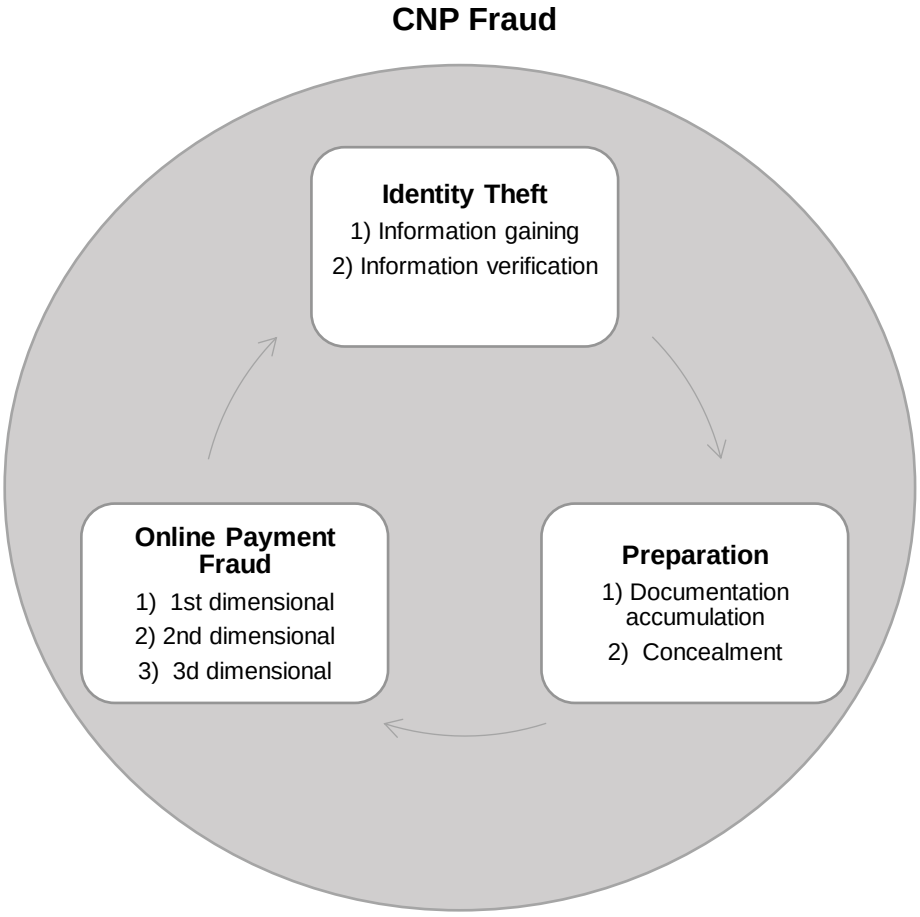

Figure 10. CNP Fraud Cycle (Albrecht & al. 2011b, 406)

The first stage of CNP Fraud cycle is Identity theft. Identity theft as a component of payment card fraud is the first step in the perpetrating the card fraud act. In order to be able to initiate an authorised online payment, the fraudster will need to seize payment card information or banking details first. This stage is a foundation upon which depends the success of the

whole illicit act. The first phase of the stage is information gaining phase, during which fraudsters need to obtain victim's private information, which can be used for financial gains further. Such valuable information might be victim's personal details, payment card details, banking credentials, etc. To obtain such information different techniques might be used. Fraudsters might search trash bins, steal mail, break into victims' homes and office as well as use internet as a tool by hacking websites, using phishing technique or skimming devices. After sensitive information is gathered starts second phase – information verification. The purpose is to check if the obtained details are valid and can be used further. One of examples of the verification could be a phone call to a victim. The fraudster can mask as an official representative of a trusty organisation and identify during the call if the stolen information is valid. Verification might take place at any other point of the process, however fraudsters who do not initiate verification of stolen information are more likely to be caught. (Albrecht & al. 2011b, 406-407.)

The obtained sensitive data can also be traded on the underground economy marketplaces. There are thousands of such sites, which are accessible only for closed criminal groups and are not easy to be tracked down for law enforcement agencies. Any sensitive information has value on the underground market and Table 2 presents some examples of prices for sensitive data in U.S. market. (Laudon & Traver 2017, 242-243.)

Table 2. Prices of stolen sensitive data on the underground economy market (Laudon & Traver 2017, 243)

Sensitive data	Price
Card number with expiration date and CVV2 number	0.5$ – 12$
Card number with full information: name, address, expiration date, CVV2, birth date, etc. (called Fullz or Fullzinfo)	30$ – 100$
Raw data: name, account number, expiration date, CVV encoded on the magnetic stripe (called Dump)	20$ – 100$
Account on online payment services	20$ – 300$
Online banking credentials	80$ – 700$
Social media account credentials	10$ – 15$
Health services credentials	10$ – 20$
Passport scan	1$ – 2$

The second stage Preparation first includes documentation accumulation step. It refers to obtaining means for perpetrating the payment fraud. For example, it can be acquiring of an identity document or payment card on victim's name that will be later used for financial gain. (Albrecht & al. 2011b, 407.) In large-scale payment card frauds OCGs are creating copies of victims' payment cards by manufacturing or buying plastic cards, on which the stolen payment card information is uploaded (Europol 2016, 29). This method is called cloning. Card cloning is a very popular documentation accumulation method, which is also often referred as counterfeit. The basic cloning approach is creating a copy of a payment card with the use of stolen card information. The counterfeit card will then be used in CP fraud. However, there are also other cloning techniques such as carding and BIN attacks that can be employed in CNP fraud. These methods involve a use of special computer programmes, which can generate sequences of payment card details. When using carding method randomly generated payment card numbers are created and then valid ones are identified and used. However, during BIN attack computer generator uses one stolen card number, which is known to be valid, and then picks-up four last numbers to create other valid cards. (Capgemini 2012, 7.)

Next step that will always take place in one way or another is concealment. Fraudsters will need to hide traces of a fraud to make sure that they are not identified and that victim does not find out about the theft for longer period. One example that the authors of the book bring out is a situation when a fraudster can change victim's email and physical address in bank's system. This way victim will not be receiving any of the bank statements sent thus the theft will go unnoticed. (Albrecht & al. 2011b, 407.) This example is very similar in nature to the account takeover technique discussed further in the chapter.

The last stage is Online Payment Fraud, during which the prepared stolen data will be put in use by making an unauthorised online payment. Payment fraud can have three possible dimensional phases. The first dimensional phase usually includes testing of the compromised payment card information. Testing in this case would be a small purchase just to check that the card is working. If the test is "passed" a fraudster moves on onto a second dimensional phase, which will include purchases of more expensive items or write-off of bigger sums. (Albrecht & al. 2011b, 407-408.) Fraudster might also be testing limits of the payment card and try to exhaust the funds held on the card by withdrawing as much as they can while the card fraud is not revealed. The third dimensional phase of Online Payment Fraud covers significantly bigger frauds that can be perpetrated when the fraudster gained confidence in the identity theft. This phase would cover such actions like opening bank account or taking a loan on victim's name. Such financial frauds are more substantial than smaller card frauds and riskier. (Albrecht & al. 2011b, 408.)

3.4.2 Identity Theft Techniques

There are plenty of identity theft techniques that fraudsters come up with constantly. Further will be discussed the most common information gaining techniques that can lead to online payment fraud.

3.4.2.1 Stolen card and Shoulder surfing

The basic identity theft technique in card fraud is a theft of the payment card itself. This method might be the most risky one for the reason that it is a physical theft. Most likely the victim will notice disappearance of the payment card and will promptly contact an issuer to block it. In such situations when card has been stolen or found fraudsters have a limited time to commit a payment fraud.

Shoulder surfing is a primitive way to steal victim's card details without physically obtaining the payment card. Fraudsters can simply see or hear payment card details, pin code or any other personal information in shops, banks, next to ATM machines or any other public places. When making a payment or cash withdrawal people should take an extra precaution and make sure that nobody can peek at their card details or other sensitive information. (Albrecht & al. 2011a, 535.)

3.4.2.2 Dumpster diving

Another way for fraudsters to obtain victims' personal information is to find documents that have been thrown away. By going through trash bins very important papers with sensitive information could be found such as bank letters with banking details and pin-codes, tax letters, receipts with payment card details, financial records, photocopies of passports, etc. For that reason, documents with any valuable information must be destroyed (shredded) before thrown away to prevent any possible identity theft.

3.4.2.3 Skimming

Skimming is a very common technique for stealing payment card information when a victim makes a purchase at POS or ATM. It involves a use of information storage device, which is called "skimmer". It could be set-up at stores, restaurants, hotels or imbedded in ATM machines (as seen on figure 11) and when a payment card has been processed the skimmer will save the card information without victim even noticing the device. (Capgemini 2012, 7.) (Albrecht & al. 2011a, 536.) Additionally to skimming devices fraudsters can install cameras at point of sales in order to record victim's pin-code. For that reason, it is advised to always cover your pin-code with a hand or wallet whenever you use it. (DFI 2015.)

Figure 11. ATM skimmer (DFI 2015)

3.4.2.4 Phishing, Spoofing and Pharming

Phishing might seem as a very primitive yet very effective way for fraudsters to deceive a victim. The primary aim of phishing is to get valuable private information by contacting a victim via email, text message, phone call, social media or via any other communication means. Scammers try to disguise their messages as official communication from authorities, banks or similar organisations to gain trust of their victims and derive private information from them to further use with criminal intentions. Such phishing emails can also contain a link to a fake phishing website, which is veiled to appear as a legitimate website of victim's online bank or any other organisation. (Capgemini 2012, 6.) Then on the website victim will be asked to update or verify their banking account, card information etc. This technique is called spear phishing (Laudon & Traver 2017, 254-255). Figure 12 demonstrates an example of phishing webpage, which implements spear phishing to obtain victim's payment card information. In the given example victim is requested to update credit card information by "Verified by Visa". Another example is shown in Figure 13, where customer of OP bank is being targeted. In this phishing page victim is requested to update online banking credentials (login and password) as well as provide personal details such as name, surname, birth date, place of birth, address and phone number. It is very crucial to remember that banks, card associations and other organisations do not request their clients to provide sensitive information via email, text messages, phone calls nor on the web pages. (OP Financial Group 2017c.) While for phishing scams it is very common to get victim's private information by request of an update of information or validation of an account. (Albrecht & al. 2011a, 536.)

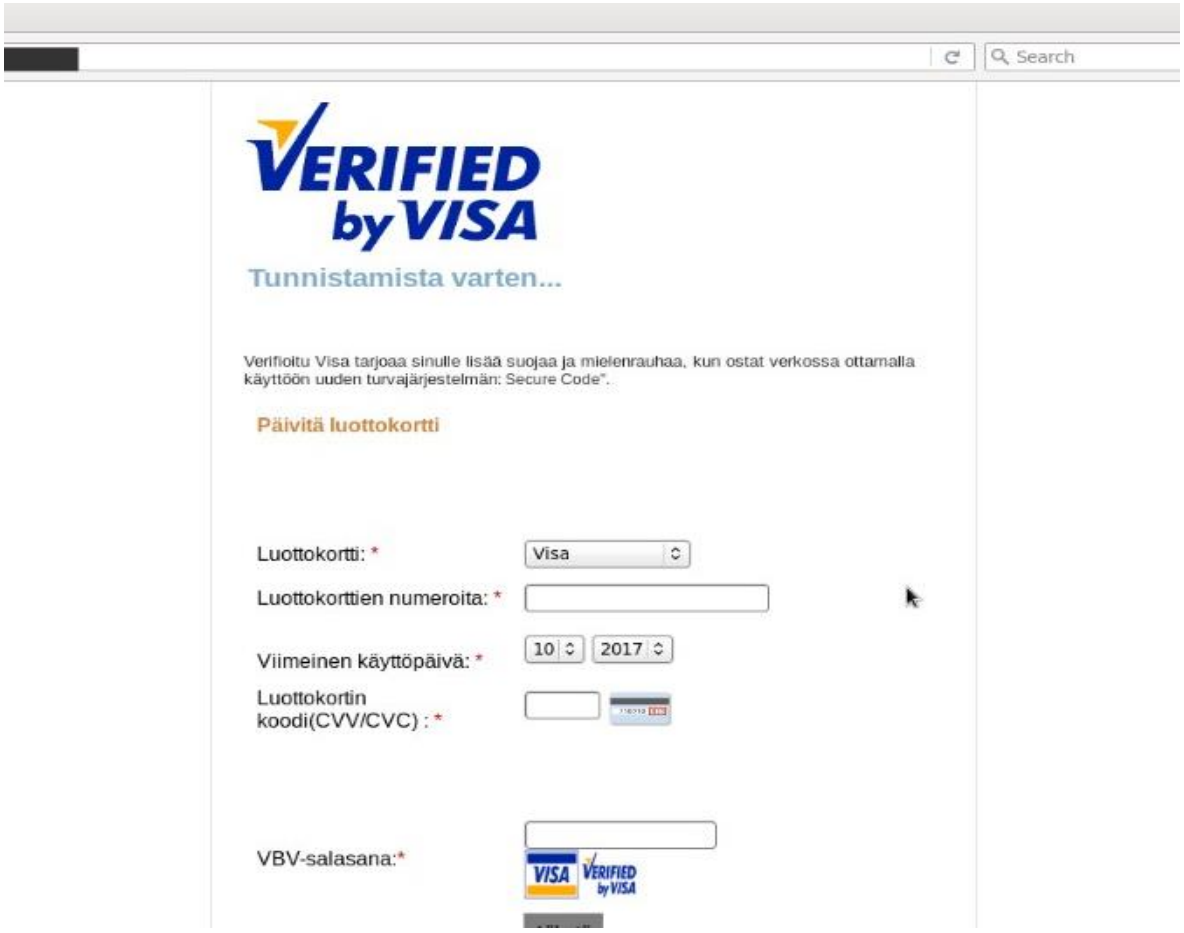

Figure 12. Example of phishing for payment card details (OP Financial Group 2017c)

If victims do not thoroughly check the email address or the website address that they have received, they can easily give out their personal information such as credit card information or their online bank credentials on the fraudulent website. The act of phishing can be classified as an identity theft, which might lead to account takeover, card payment fraud or to any other criminal acts depending on the goal of the scammers.

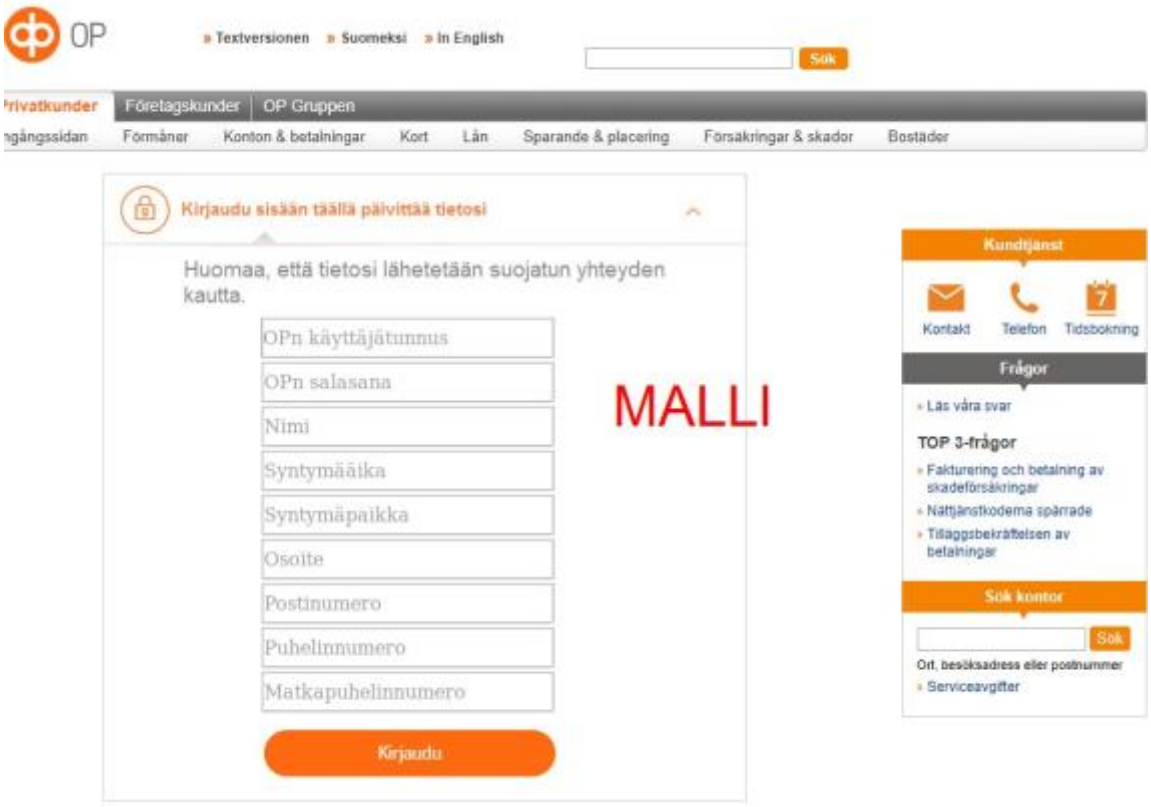

Figure 13. Example of phishing webpage (OP Financial Group 2017e)

OP Financial Group advises to its customers to check that the webpage address contains “httpS” (Figure 14). “S” stands for security and means that the site is protected. As well as presence of a lock sign is very important. It indicates the legitimacy of a website – weather the website certificate is granted to OP Financial Group companies or not. (OP Financial Group 2017b.)

Figure 14. Example of legitimate OP Financial Group websites (OP Financial Group 2017b)

What can make phishing even more deceiving for victim is spoofing technique. This technique involves using real e-mail or IP addresses. Fraudsters are able to mask their email address as somebody else's e-mail address and send their phishing messages from this spoofed e-mail. This technique allows to gain absolute trust of victims, who will think that the e-mail is coming from an authorised sender. Same applies to IP addresses, when fraudsters create IP packets that use someone else's IP address to appear as a legitimate host. Quite often a web site can also be spoofed in combination with a pharming method. Pharming is redirecting victim to a spoofed web site when they are clicking on a link, which was supposed to lead to a legitimate site. (Laudon & Traver 2017, 261.) Such technique can easily be used to scam buyers on spoofed e-commerce web sites by collecting their card information at check out.

3.4.2.5 Malware and PUPs

Malware is one of the most popular fraud techniques nowadays that according to the theory studied earlier belongs to sub-category of hacking in internet crimes. In a nutshell malware is a malicious software - computer program, which is created with fraudulent intentions. (Gottschalk 2010b, 22.) Malware brings such threats like viruses, worms, Trojan horses, ransomware and bots (Laudon & Traver 2017, 250). Such malicious agents can attack and gain control over operating system, database, network or computer on behalf of a fraudster. They are aimed to collect any sensitive information of victims such as passwords, personal information, payment card detail, etc. Malwares can be very advanced and can automate numerous attacks. Such fraud poses a big threat and contributes to rising number of financial internet crime every year. (Gottschalk 2010b, 22.)

Potentially Unwanted Programs (PUPs), which usually contain malware, is a substantial threat for internet users' private information. As a rule victims are fooled into downloading this malicious applications on social networks and websites where upon the PUPs will install themselves on victims' computers even without their consent. Furthermore they are not easy to be removed from computer once installed. The PUPs and their purposes can be diverse. They may gain control over the computer and lead to disabling security software and infecting computer with even more malware. With the use of browser parasite criminals can manipulate victim's browser. Such PUP might not only track visited pages, but if very advanced might also steal passwords and any sensitive information (including card data) that was input in the browser. Another dangerous PUP is a spyware, which is designed specifically to collect private information like e-mails and messages, record keystrokes and take screenshots to steal any valuable data. PUPs are very effective criminal tools for identity theft. (Laudon & Traver 2017, 254.)

3.4.2.6 Sniffing and Man-in-the-middle attacks

Sniffing is a technique that involves use of an eavesdropping programme that can scan network for information. It can be used with legitimate objectives to identify problems in network or track criminals. However, when utilized by hackers the technique is used for any sensitive data theft including passwords, card information, private files etc. The eavesdropping programme called sniffer allows fraudsters to track down any information that is moving in a network and steal it. When used with fraudulent intentions sniffer is very damaging and difficult to detect. For example in year 2013 U.S. corporate networks of retail chains have been targeted with the sniffing programmes. Over 160 million credit card numbers have been stolen as a result of this attack. (Laudon & Traver 2017, 262.)

Sniffing can also be targeting e-mail communication. Such type of sniffing is called e-mail wiretaps. Hackers can also intercept in such communication between two parties and control it. This attack is known as man-in-the-middle and allows fraudsters to gain benefit by misleading parties involved into the communication. (Laudon & Traver 2017, 262.)

3.4.2.7 Data breach

Data breach is a leak of corporate information to outsiders as a result of lost control over internal system. Data breaches inevitably lead to the identity theft in big volumes. The biggest reason behind the data breaches are hackers with fraudulent motives. Such hacker attacks for example have accounted to almost 50% out of all data breaches in U.S. in year 2014 and led to compromising 75% of identity information. 22% of breaches were due to the accidental information disclosure and 21% resulted from computer stealing. (Laudon & Traver 2017, 259.) The same year in Finland cyber-attack has targeted IT company Arc Technology. The aim was the server, which was used by 8 big companies including VR, to login into HR information system. The system contained such data as employees' names, social security numbers, and salary details of thousands of workers. It was not evident if the theft of personnel's sensitive information has occurred or not, but investigation showed that the hackers gained control over login server in order to distribute spam emails and use it for similar fraudulent activities. (Yle uutiset 2014.) Nowadays the systematic system hacking leads to the most cases of card fraud. When fraudsters target e-commerce sites, where millions of card purchases are stored, they easily get their hands on a big chunk of card data at once. (Laudon & Traver 2017, 260.) All organisations need to execute an adequate server security and precautious in order to avoid data breaches, which can compromise their clients' information.

3.4.3 Online Payment Fraud

Once payment card information has been collected with the use of identity theft techniques or purchased from another criminal group, then fraudsters move on to committing online payment fraud (trial stage) by simply making purchases in e-commerce stores.

One of variations of online payment fraud is account takeover. The technique involves fraudster gaining control over victim's account in e-commerce website or even in online banking system. Account numbers and passwords are obtained with the use of any of the identity theft techniques that are studied earlier in this chapter. Then a fraudster will change the personal information of the victim in the account such as e-mail address and home address and will use the provided card details for making purchases. After the unauthorised purchases are done it might take some time for the victim to find it out and identify the account takeover. (Capgemini 2012, 6.)

4 CNP Fraud in EU and Finland

Payment card fraud is an exceptionally profitable and a low risk illicit activity. It is run by organised crime groups (OCGs), whose actions have disturb security of card transactions and cause big losses in Europe. As reported by Europol the yearly profit of European OCGs from card fraud activities reach 1.5€ billion. (Europol 2012, 3.) This number is supported by the "Fourth report on card fraud" published by ECB, which reports 1.44€ billion in losses related to card fraud in year 2013 (European Central Bank 2015, 7.) This income has been growing from year to year and further has been used in the card fraud activities, for example invested in technical equipment and developments. The OCGs are also investing into other illegal enterprises and putting their incomes into money laundering. (Europol 2012, 3.)

Below is presented statistic provided by ECB that demonstrates a breakdown of card fraud value in Europe by type: POS (CP) fraud, CNP fraud and ATM fraud. Starting from 2009 CNP fraud is accounted for over 50% every year out of total card fraud. In 2013, this figure reached the mark of 66%, which makes CNP fraud the major card fraud type among other. While CNP fraud has been constantly rising from year to year, CP and ATM frauds on the contrary have been decreasing. CP fraud dropped from 36% in year 2008 down to 20% in 2013. A similar tendency can be noticed with ATM frauds, which totalled to 18% in 2009, then were fluctuating during the past years and in 2013 dropped down to 14%. On average CP fraud exceeds ATM fraud only by 6% in the last three years. These figures allow to draw a conclusion that CNP is the biggest growing threat for security of payment card industry in Europe that alone totalled to 958 million euros in 2013. (European Central Bank 2015, 7.)

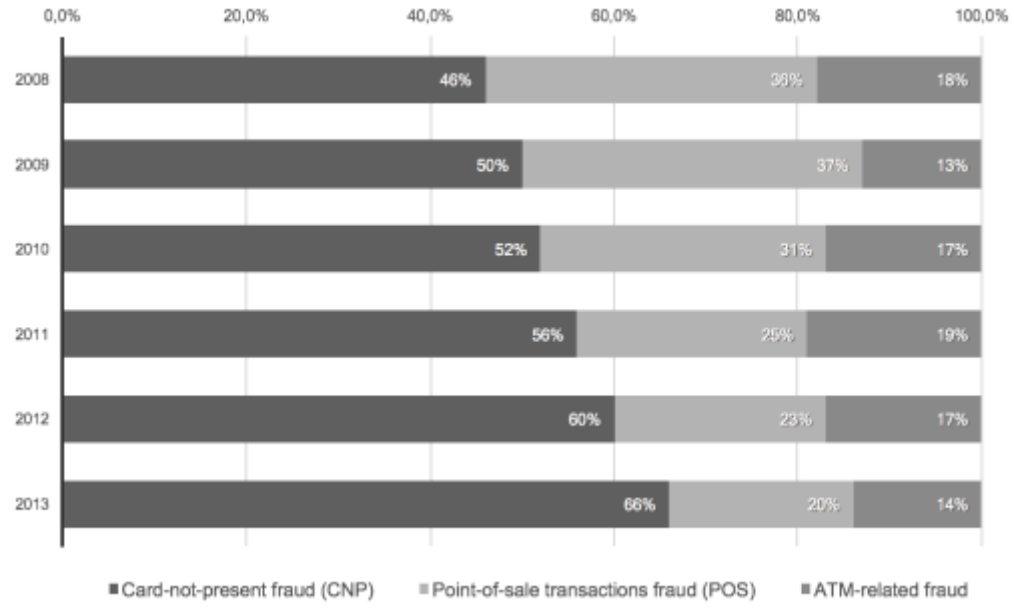

Figure 15. Breakdown of card fraud value by type 2008 - 2013 in Europe (European Central Bank 2015, 7.)

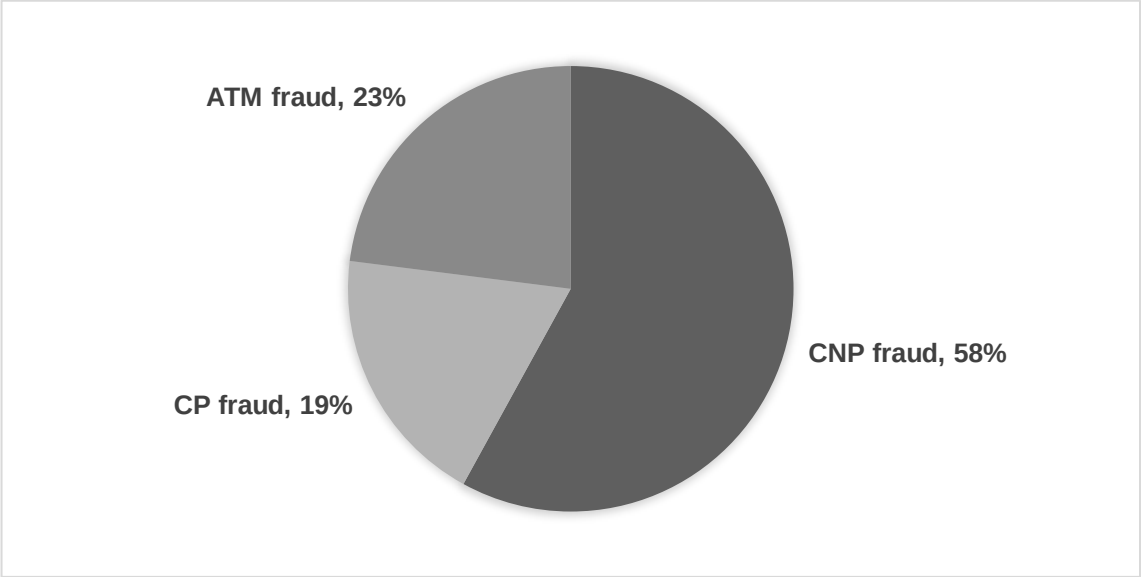

Figure 16. Breakdown of card fraud value by type in 2013 in Finland (European Central Bank 2015, 22.)

Statistics from Finland (Figure 16) present a slightly different distribution between CP and ATM fraud. In year 2013 ATM fraud outweighs CP payment fraud by 4% in the country. This can indicate that ATM machines are easier fraud targets rather than physical point of sale. However, the situation with the major fraud type is same as in the rest of Europe. CNP fraud, which totalled to 58% out of all card frauds in 2013 remains the key threat for security of card payments.

Such growth of CNP fraud can be explained by rising amounts and volumes of CNP transactions. CNP transactions in Finland have been evidently growing. Statistics from Bank of Finland (Figure 17) show that number of remote transactions has increased from year 2015 to year 2016 by over 14 million transactions. It is a noticeable rise in comparison to growth of only 3.25 million transactions that occurred year earlier in 2015. In terms of CNP volumes there has been a corresponding increase of 0.52€ billion in 2016 (Figure 18). It is a big boost for Finnish economy. Previous year to that resulted in only 0.08€ billion rise. (Bank of Finland 2016.) Such increase in CNP transactions can indicate a rapid growth of e-commerce industry in Europe. For that reason, an overview of B2C e-commerce growth in Europe and Finland has been provided in the next sub-chapter.

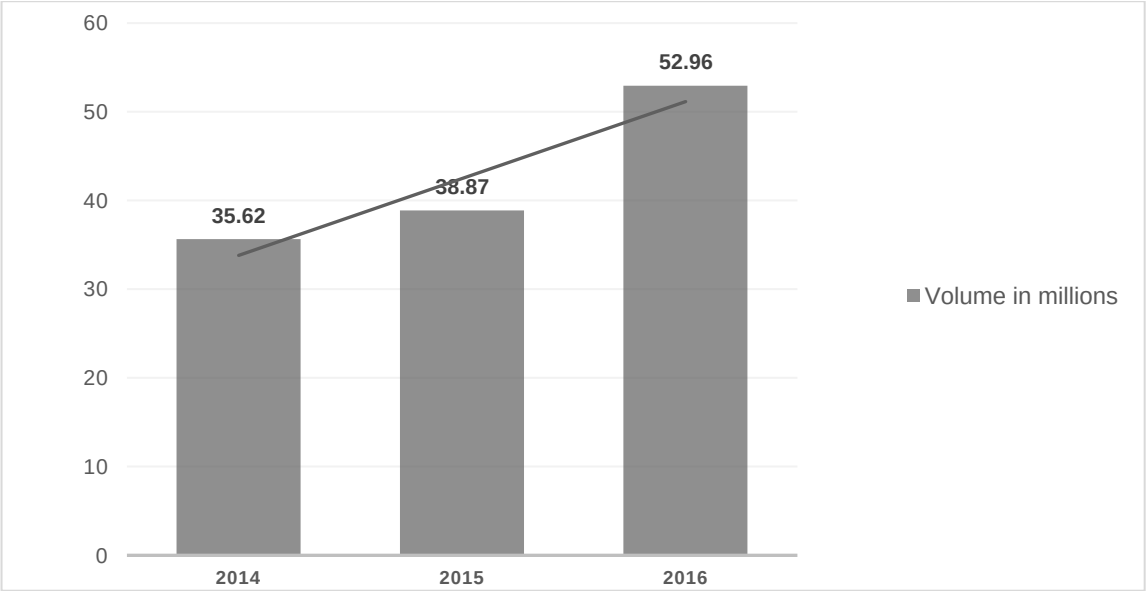

Figure 17. Number of CNP transactions in Finland 2014-2016 (Bank of Finland 2016)

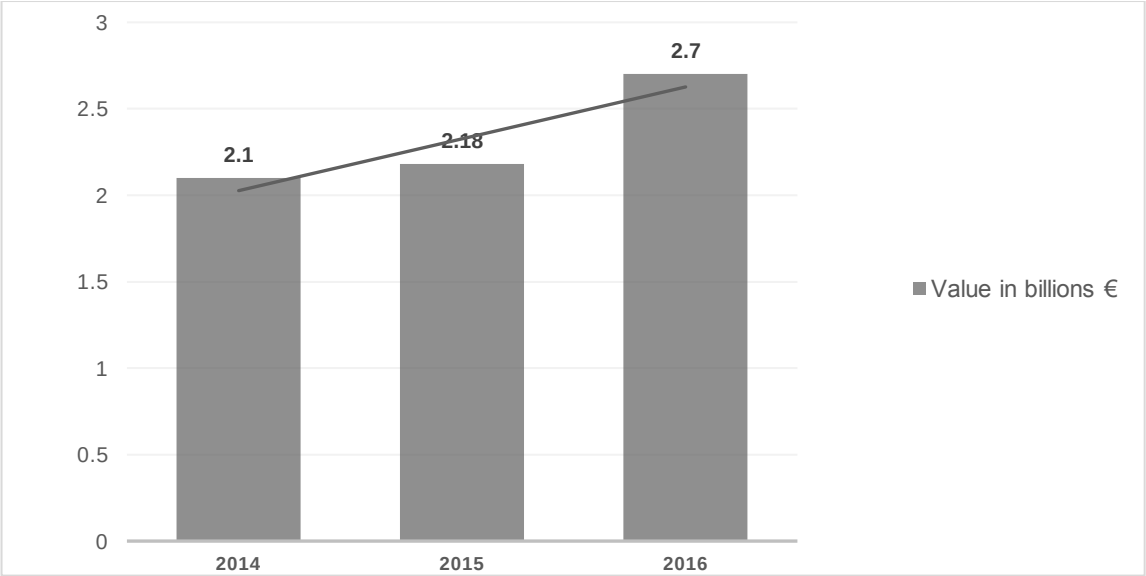

Figure 18. Value of CNP transactions in Finland 2014-2016 (Bank of Finland 2016)

4.1 E-commerce growth in Europe and Finland

B2C e-commerce industry and its trends are analyzed with the use of statistical reports from statista.com and ecommercefoundation.org alongside with other sources.

Global statistics on number of online consumers (Figure 19) represent the worldwide tendency in the industry: more and more people are making their purchases online. From year 2014 to current year 2017 the number of online buyers has increased from 1.32 billion to 1.66, accounting for 25% in growth rate. According to the forecast (f) it can be expected that the number of online buyers will continue growing and will reach 2.16 billion by year 2021.

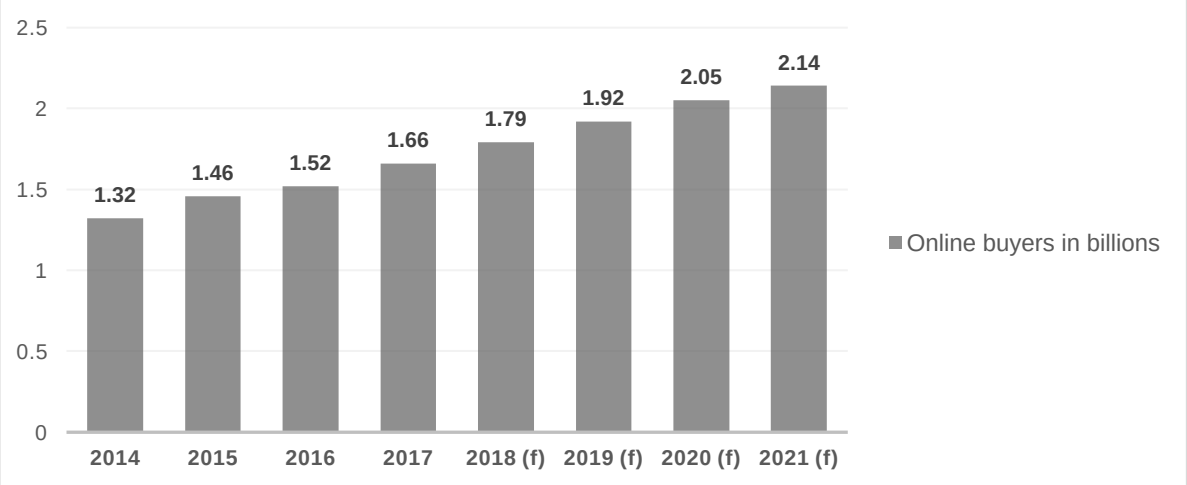

Figure 19. Number of online buyers worldwide 2014 – 2021 (Statista 2017d)

One of the contributing factors to the growing number of online buyers is a growth of internet penetration in the countries. In Europe internet coverage expands annually (Figure 20) and Northern Europe takes the lead with 93% internet penetration in 2016. (Ecommerce Foundation, 26)

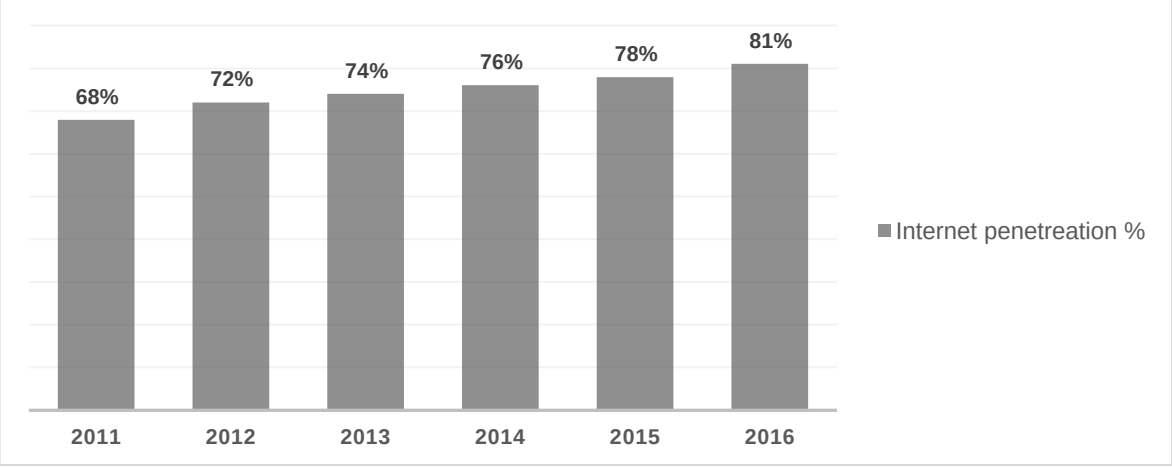

Figure 20. Internet penetration in Europe 2011-2016 (Ecommerce Foundation 2017)

A higher amount of buyers leads to higher volumes in the money flow. In Europe the sales from e-commerce activities have amounted to 530.58€ billion in year 2016 and will reach 602.84€ billion already this year (Figure 21).

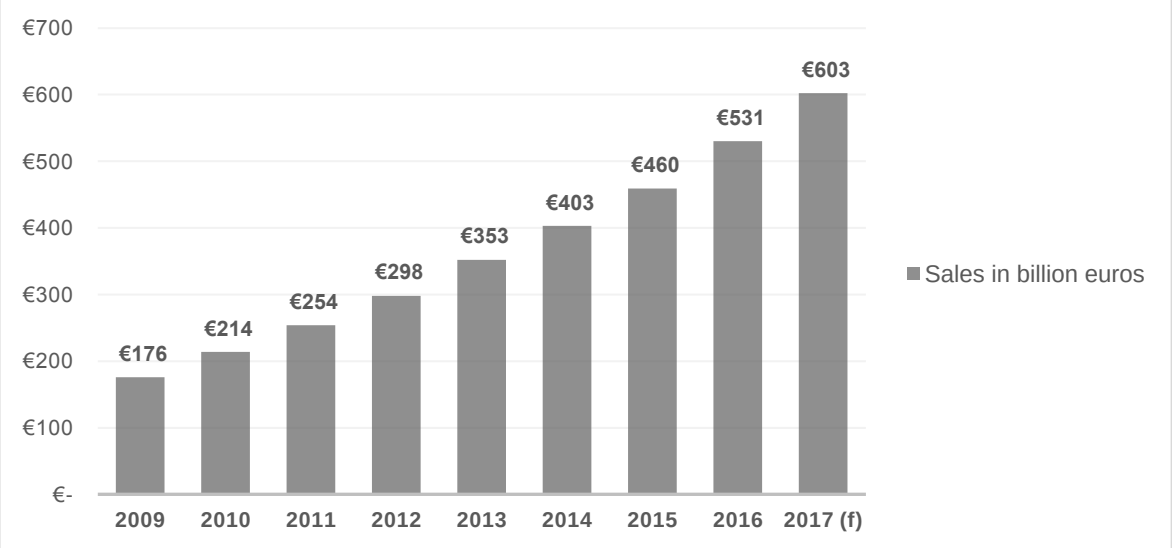

Figure 21. B2C e-commerce sales in Europe 2009- 2017 (Ecommerce Foundation 2017)

Even though the Nordic countries do not hold the biggest e-commerce market share, they still contribute quite a lot to the e-commerce sales among the European countries. The below chart represents the average annual spending per capita in Europe when shopping online. From the chart it is clear that consumers from Northern Europe (Finland, Sweden, Norway, Denmark and Iceland) are third in Europe according to their average annual spending online.

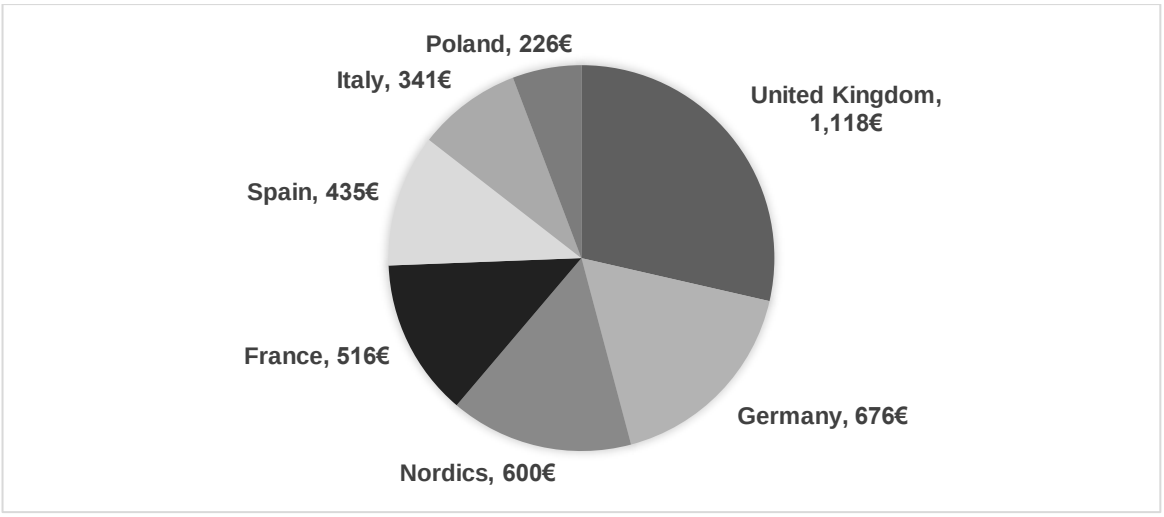

Figure 22. Average annual spending per capita for online shopping in Europe in 2016, by country (Statista 2017a)

Finland has been among the countries that spend quite a lot on online purchases (Figure 22) and the spendings grow yearly. It can be clearly seen from the below presented growth of e-commerce payment volume in Finland over the years (Figure 23). The statistics show that from year 2014 to year 2016 index of online payment volumes has risen by 90, which means that only in two years the volume of e-commerce payments almost doubled.

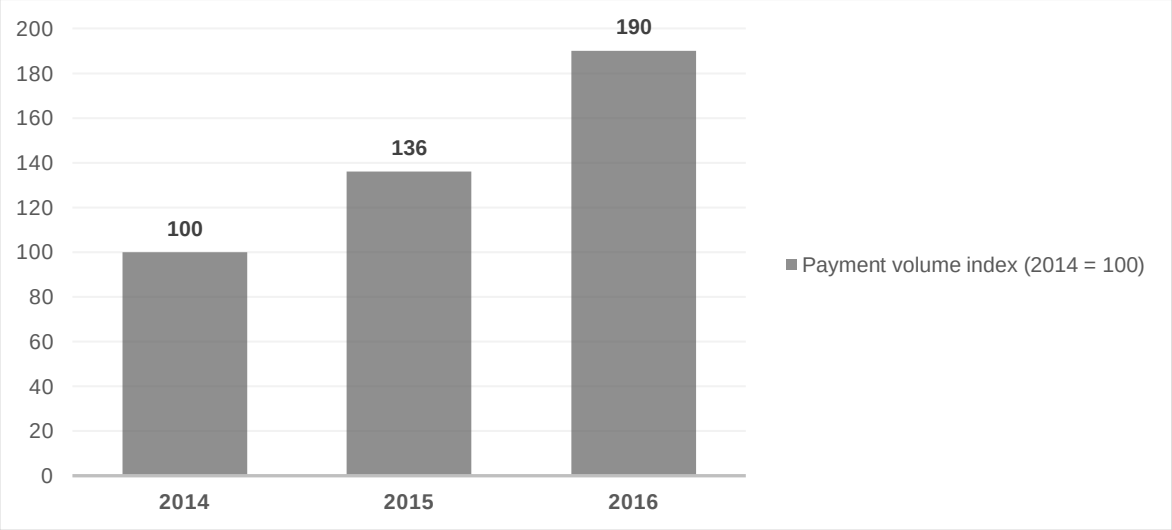

Figure 23. E-commerce payment volume index growth in Finland 2014 - 2016 (Statista 2017b)

All the presented trends in the B2C e-commerce industry clearly indicate a constant growth of online shopping all over the Europe and particularly in Finland. Bigger amounts of online consumers and higher volumes in sales in e-commerce bring more opportunities for the Financial Internet Crime. It can be assumed that payment cards would be the number one target for the fraudsters due to the fact that they are still the most common online payment method among the buyers. That can be proven for example by the results of the survey, which has been conducted among respondents from Northern Europe (Finland, Sweden, Norway, Denmark and Iceland). Findings of the survey present the most preferred payment method online (Figure 24). Payment with the use of debit and credit is the most popular payment choice, which is accounted to 35% out of the total responses in Nordics. Wires through online bank (18%), PayPal (19%) and use of invoices (21%) are less favourite payment methods.

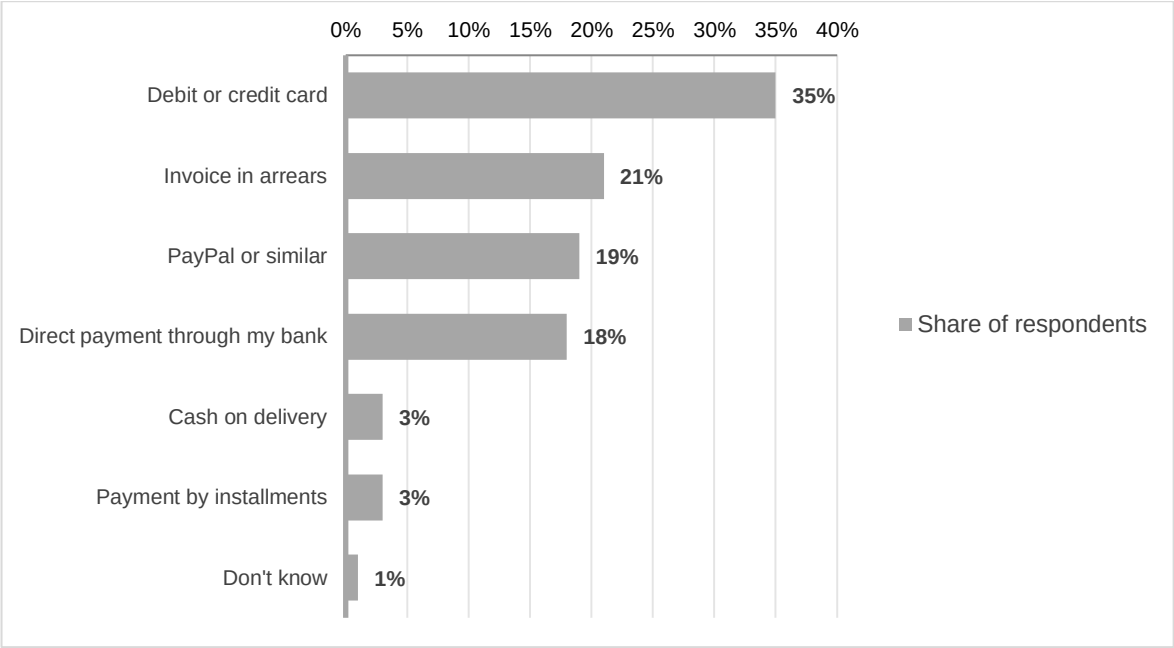

Figure 24. Most popular payment methods for online purchases in the Nordic countries in 2016 (Statista 2017c)

5 Card Fraud Prevention

Based on the studied CNP fraud process and its techniques it can be concluded that in order to prevent CNP fraud from occurring two critical points must be addressed: prevention of card data theft and prevention of unauthorized CNP transactions. Next will be discussed the existing and new card fraud prevention methods that have been implemented in financial services industry.

5.1 Prevention of card data theft

Identity theft is the first phase in a CNP fraud, which must be prevented. To avoid card data theft and card counterfeit the following discussed methods have been implemented in card industry in the recent years.

5.1.1 EMV chip

For prevention of card counterfeit the EMV chip, which stands for its promoters Europay, MasterCard and Visa, has been introduced around year 2006 and has been fully implemented since then on territory of Europe. This chip is a computer chip, which is embedded in a payment card. It is meant to replace the old magnetic strip, which was in use since year 1970 and was fairly easy to clone. A payment card with the EMV chip is using cryptography for payment authentication and PIN code or signature for customer identification during CP transactions. The key advantage of the EMV chip is that it is made to be more difficult to copy and steal card information from it than from a magnetic strip. Cards with EMV chip are also referred to as smartcards or chip cards. (Communications of the ACM 2014, 24; Laudon & Traver 2017, 260.)

Figure 25. EMV chip

Figure 26. Magnetic strip

However, not all POS and ATMs have been updated with the EMV technology yet. A lot of countries outside Europe are still migrating towards EMV environment. For example in year 2015 U.S. were still in the middle of EMV implementation. (Laudon & Traver 2017, 260.) And for that reason even European payment cards are still manufactured with the magnetic stripe and the EMV chip at the same time. This results in fraudsters taking advantage of this situation by stealing card data of EU cardholders and utilizing it at POS and ATMs that are non-EMV compliant outside the EU zone (European Central Bank 2014, 39). The ideal solution for the problem would be a global implementation of EMV technology at some stage. However, the temporary action that has been taken is producing cards that have magnetic stripes, which must be activated when travelling outside of EU zone. This method allows the use of the payment card only at POS and ATMs that are compliant with EMV standard, but will also work with magnetic stripe if it is activated. This way card fraud can be prevented from occurring in the areas outside the Europe that are still lacking EMV terminals. (Europol 2012, 7-8.)

It can be concluded that EMV chips are effective for identity theft prevention as they are protected against card skimming, as well as for card fraud prevention in CP scenarious at POS and ATMs, because they require a PIN code. However, the weak point of the chip cards currently is the fact that they are stil being manufactured with the magnetic strip, which can be exploited outside of Europe with the use of non-EMV terminals.

5.1.2 Tokenisation

Another method for protecting card information from being stolen is tokenisation. Tokenisation is a technique, which algorithmically generates series of random numbers called token. There are various ways how tokenisation can be used for example in online

banking as a one-time login password or as a payment authorisation code. (Square Inc 2017.) However, in card payment industry tokens can replace card numbers when making a payment. This way the sensitive card information is not exposed thus the risk of card fraud is avoided. Tokens can be used in e-commerce environment when making a CNP payment, but also at physical POS when using mobile payment. Tokenisation technology is incorporated in such mobile applications like Apple Pay and Android Pay. (Visa Europe 2017a.) To initiate a payment token number will be sent by card issuer to cardholder, who will provide it to card payment acceptor. The token number will be routed same as card data would normally do during authorisation process. Card network will use its token vault to identify the cardholder's account number and will forward the information to issuer for authorisation. (PaymentsCM LLP 2015.)

To protect its clients from card fraud Visa has launched tokenisation service in Europe in year 2015. Now Visa clients are able to use secure digital tokens on their devices when making payments in stores and online. Introduction of tokenisation for card data security is considered as a big advancement in card fraud prevention. (Visa Europe 2017c.) It is a better alternative to payment cards, because cards transmit card details in the network that can be compromised along the way. Whilst tokenisation uses tokens, which are not revertible to the original card number. For example, in case of a data breach of e-commerce site fraudsters will only discover token numbers instead of card data stored. (PaymentsCM LLP 2015.)

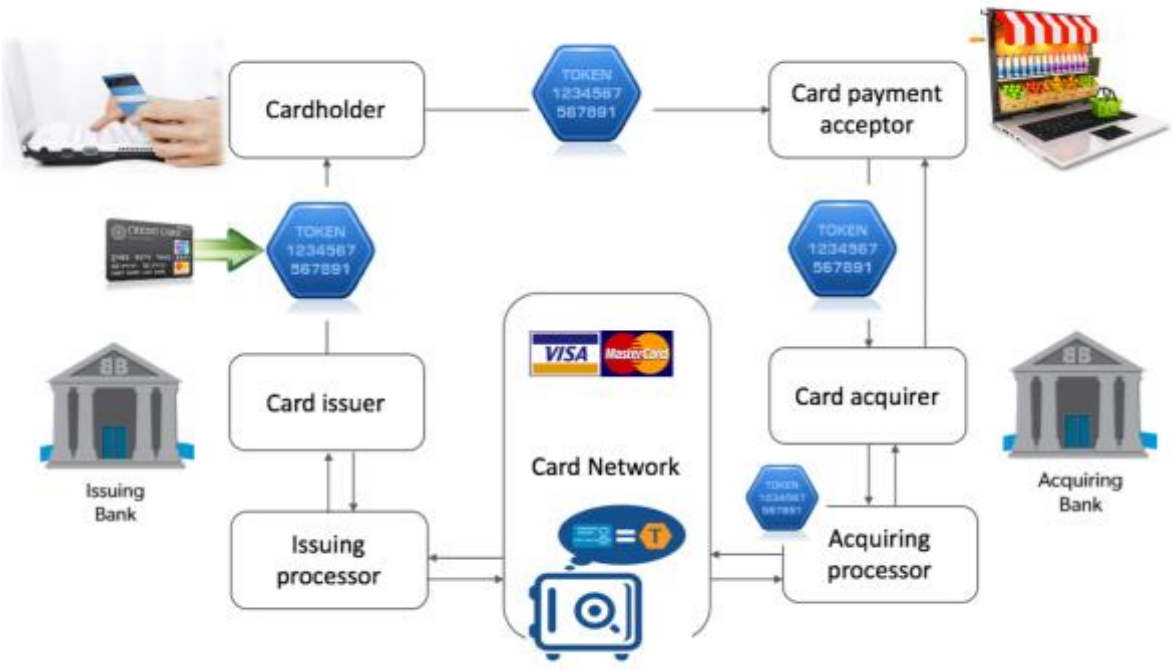

Figure 27. Authorization process with involvement of tokenization (PaymentsCM LLP 2015)

5.2 Prevention of unauthorised CNP transactions

If card data has been already obtained by fraudsters it is crucial to prevent the payment fraud from occurring. A very important component of card fraud prevention in financial services industry is presence of good fraud mitigation methodologies. They allow to identify fraudulent transactions and prevent them promptly. It is a very critical and very important point during authorisation process (see subchapter 3.4.2.). Further the most popular fraud mitigation methodologies are discussed. (Capgemini 2012, 12.)

5.2.1 Analytics

A crucial tool that has been employed by financial services institutions for identifying fraudulent transactions is analytics. Analytics work by first creating portfolios of each cardholder. Fraud specialists will analyze regular spendings of a cardholder and as a result will create a set of rules for each portfolio. The rules can cover such characteristics of transactions like their size, nature of payments, location of POS or website, intervals between transactions, etc. If in future processing transaction does not comply with the set rules of the portfolio, then it will be flagged during the authorization process and additional authentication from cardholder will be required. After portfolio has been created it will be updated regularly to track any pattern changes of cardholder's spendings. Portfolios can also be grouped based on similar spending patterns of cardholders and will be monitored together. (Capgemini 2012, 12.)

5.2.2 3D Secure

Prevention of unauthorized transactions in e-commerce environment requires security of online payment environment as well as supplementary identity authentication of card holders. For this purpose European card industry has introduced a 3D secure protocol: verified by VISA, MasterCard secure code. (Europol 2012, 3, 11.) 3D secure is an additional payer authentication, which is supported by three parties: online merchant, who has adopted the protocol, card acquirer and card issuer (Get Elastic Ecommerce Blog 2017.) This authentication works by asking a cardholder an additional question or password at the checkout (Visa Europe 2017d). The cardholder has to be also registered at the verified by Visa or MasterCard secure code. If the customer was not registered prior to the purchase on the website, which supports 3D secure protocol, he will be redirected to the enrolment page. This method protects merchants and cardholders against unauthorised transactions and the potential losses (Get Elastic Ecommerce Blog 2017.) Unfortunately, 3D secure protocol is not an accepted standard for CNP transactions thus it is not used by all online merchants and cardholders even within the EU zone (Europol 2012, 11).

5.2.3 Biometrics

Use of biometrics is a new approach in payment authentication process that is coming as an alternative for 3D Secure service. Biometrics is a technology, which allows to perform person's identification with a use of his biological features such as fingerprints, facial features, voice and iris (Nasdaq 2017).

MasterCard has already released a new application for smartphones called Identity Check Mobile, which incorporates biometrics into cardholder authentication. The technology identifies cardholders with a use of biometrics such as fingerprints and facial recognition. Instead of inputting a passcode to authorise a payment, cardholders will be sending a fingerprint or a photo of themselves in real time. This will not only improve customer experience during online payment, but most importantly strengthen cardholder's authentication and reduce online payment fraud. Identity Check by MasterCard has been introduced in twelve markets in Europe including Finland during year 2017. (MasterCard 2017.)

5.2.4 Geo-blocking

Combating payment card fraud has always been a big challenge for European Union's authorities. The OCGs are usually very complex and wide spread organisations all over the world. Quite often card fraud activities are performed outside the European Union, but will affect cardholders inside the member states. The fact that the card fraud perpetrated is cross-border makes it very difficult to track and investigate the crime. Another complication is inability of law enforcement agencies like Europol to cooperate with non-European police authorities when investigating cross-border card fraud cases due to the legal and organisational limitations. (Europol 2012, 5-6.) This indicates a strong need for card fraud prevention methods that will target international aspect of the crime.

One of such card fraud preventive methods is geo-blocking. Geo-blocking is an additional card security service that can be offered to cardholders by card issuers. By enabling this service cardholders can limit certain countries, where their payment card will work. It means that if any transactions are initiated in the restricted by a cardholder area, they will be rejected. This provides protection in cases when card data was compromised and used abroad. When travelling outside home country cardholder can change the geo-blocking preferences. Geo-blocking does not apply onto CNP environment, however restricting online payments is possible. Cardholder can practice switching online transactions on when doing any online payments and switching them off when not doing any. (Danske Bank Group 2017f.)

5.2.5 Security limits

Security limits are usually being set by banks or by cardholders themselves on daily CP and CNP payments and on cash withdrawals from ATM machines. They define the volumes of funds that can be used in one day with a payment card. Security limits are not directly preventing card fraud, but they play a role of an additional tool to mitigate losses from already occured misuse of a card by restricting the amounts that fraudsters can withdrwal.

Importance of security limits on various payment types can be seen in Figure 28, which presents my personal bank account on the moment of CNP fraud. As daily payment limits were not applied on the card, fraudsters were able to initiate multiple unauthorised transactions of high value. Daily security limits would have helped to minimise the losses. However, taking into consideration that such big payments and especially in Indian currency were not part of my typical spending habbits rises a question: why the bank did not consider such payments to be suspicious?

Tiliote 1 (1)
Ajalta 1.2. - 29.2.2016
09.03.2017

[redacted]

KÄYTTÖTILI

Tilinumero [redacted] BIC: OKOYFIHH

Kirjaus-päivä / Arvopäivä	Määrä euroa	Selitys / Maksunsaaja/maksaja/viesti	Viite	Arkistointitunnus / Saajan tilinumero / Saajan pankin BIC
	[redacted]	SALDO 31.1.2016		
3.2.16 3.2.16	-3 182,90	PKORTTIMAKSU BOLLYWOOD EXPRESSIO JALANDHAR Viesti: [redacted] OSTOPVM 160202 INR 230000,00 KULUT 0,00 VAIHTOKURSSI 1 EUR = 72,2648 INR MF NRO 7439173603400000910859 9 VARMENTAJA 050		201602035EQEL2006982 J
3.2.16 3.2.16	-1 257,94	PKORTTIMAKSU BOLLYWOOD EXPRESSIO JALANDHAR Viesti: [redacted] OSTOPVM 160202 INR 90900,00 KULUT 0,00 VAIHTOKURSSI 1 EUR = 72,2648 INR MF NRO 7454485603460332275357 9 VARMENTAJA 050		201602035EQEL2006983 J
4.2.16 4.2.16	-372,22	PKORTTIMAKSU BRAHMANAND AYURVEDA JALANDHAR Viesti: [redacted] OSTOPVM 160202 INR 27000,00 KULUT 0,00 VAIHTOKURSSI 1 EUR = 72,5426 INR MF NRO 7454362603460333017629 0 VARMENTAJA 050		201602045EQEL2006782 J

Figure 28. Bank statement with three unauthorised transactions

5.2.6 Alerts

To ensure that cardholders are aware of all processed transactions financial services institutions can offer such service as alerts. It can be a notification by SMS or e-mail of every transaction occurred or of transaction above certain limit. Alerts are not only a good way to track own spending for cardholder, but also an efficient tool for fraud mitigation. In some cases banks can call to a cardholder to confirm that transaction was initiated by cardholder. Even though the alert will be received by cardholder only once the authorization process has ended (meaning that an unauthorised transaction was not prevented), the financial institution still can block payment before settlement process starts. It can be done in case when the merchant, who is claiming the payment is fraudulent, and when the payment was done without cardholder's consent. For that reason alerts are very crucial tools since they help cardholders to spot unauthorized transactions in time and contact their bank immediately. (Capgemini 2012, 12-13.)

5.2.7 Device tracking

Device tracking is a fairly new technique for payment fraud prevention. It works by tracking the known devices of cardholder when payments are done. If any transaction will be initiated from new unknown for the programme device, then the transaction will be flagged and the cardholder will be contacted directly. In case of unauthorised transaction the fraudster's device will be blocked for any further transaction attempts. (Capgemini 2012, 13.) This solution seems to be very effective for fraud prevention.

Another great fraud preventive service that started to be offered by banks to their clients in year 2015 is tracking of clients' mobile devices with a purpose to identify location of cardholder during initiated payment transaction. It is presumed that cardholder's mobile device is almost always present with him. This way transactions that have occurred in a different location than cardholder's mobile device's geo-location will be assumed to be fraudulent and will be stopped. This is not only a great tool for identifying unauthorised transactions, but also a way to improve customer satisfaction. Quite often banks' clients might complain about their transactions being rejected while travelling. It happens when a bank was not informed about client's plans to go abroad or geo-blocking was not deactivated. In any way with the new service of authorizing transactions with the use of matching client's mobile device's geo-location and geo-location of initiated payment, such instances of declined transactions during travelling should be minimised as well as the payment card fraud. (Visa 2015.)

6 Research Design and Research Methods

The main goal of the research is to learn how the studied card fraud threats are being addressed in real life by banks and answer the research question “How do banks prevent card fraud?” To answer this question it was decided to conduct a case study with three case banks: OP Bank, Nordea Bank and Danske Bank. These financial institutions are well-known Finnish and Nordic banks and were selected based on that fact that they are rated as top leading banks on territory of Finalnd (Corporate Finance Institute 2017). As leading banks in the country it was assumed that the organisations provide their customers with the most progressive services and methods for card fraud mitigation. For this reason, it was decided to analyse card fraud prevention services of these particular banks.

The first part of the research is answering to the IQ 1. “What card fraud prevention services do banks provide?” It involved collecting data on card fraud prevention services and methods, which are currently available in the case banks for their clients. The services are aiming to prevent card fraud from occurring and to minimise losses associated with it.

The data has been collected directly from official websites of the case banks. The websites were used as primary data sourses because they were easily accessable for me and contained all the neccesary up-to-date data to answer research questions. During data collection process I have searched websites for information on card fraud prevention services and methods that are available for cardholders in the banks. Not all banks have a separate section dedicated to card fraud on their pages, but the information was mainly spread in different parts of websites. That fact made it a bit more complicated to gather all pieces of information. All the collected data is presented and evaluated in chapter 7. “Banks’ services for card fraud prevention”. Since I was able to answer to the research question with the use of the information obtained from the banks’ websites it was decided that it is not necessary to conduct additional interviews.

In the second part of the research the collected data from the first part has been used. I have compared the existing card fraud prevention services provided in the selected banks with the card fraud prevention methods studied in theoretical chapter 5 “Card Fraud Prevention”. The comparison was summarised in a form of table to make it more visual for a reader (see Table 4). This analysis allowed to identify what card fraud prevention services that are available in the industry the case banks could adopt and how the existing methods can be developed. This way the IQ 2. “How can banks develop fraud mitigation services?” has been answered. The findings of this reserch part are presented and discussed in chapter 8 “Results”.

The end result of the study will be a review of card fraud prevention services and methods, which are currently provided by the case banks, and recommendations on how they can be developed. The overview of the research design is presented in Figure 29.

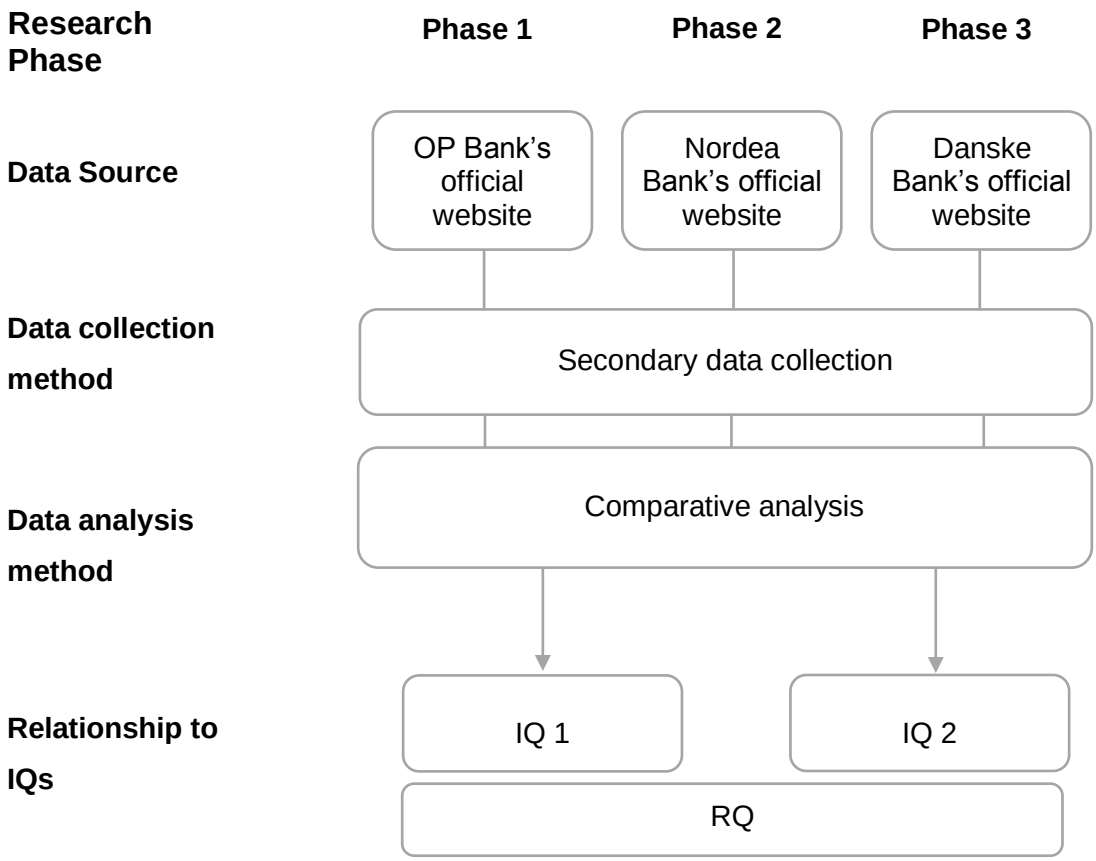

Figure 29. Research design

7 Banks' services for card fraud prevention

In this chapter, the case banks will be introduced and it will be examined which card fraud prevention services are available for the banks' clients.

7.1 OP Bank

OP Financial Group is the largest financial services group in Finland that includes around 180 member cooperative banks all over the country. The OP banks are independent deposit banks, which operate locally. Analogous retail banking services in Helsinki area are provided by OP Financial Group Central Cooperative's wholly-owned subsidiary Helsinki OP Bank Ltd. Customers of the OP banks are private clients, small and medium enterprises, forestry and agricultural customers and public sectors. (OP Financial Group 2017d.) In year 2016 the organisation has reported 160 billion US dollars of assets and 1,370 million US dollars of net income (Corporate Finance Institute 2017).

All payment cards issued by the financial institution have been compared and it was found that the card fraud preventative services that are offered by OP banks are: 3D Secure, security limits on payments and payment alerts. Further is presented information on the services collected from the bank's website (uusi.op.fi).

OP bank is issuing both Visa and MasterCard payment cards with debit and credit options. All of them have an embedded EMV chip and 3D Secure protection: Verified by Visa and MasterCard SecureCode. The only card, which does not have a 3D Secure service is a Visa Debit Mobile, which is a card that is designed specifically for contactless payments at physical points of sale with a use of phone. (OP Financial Group 2017a.)

Security limits on the payments are available for all cards issued by OP bank. Cardholders can set suitable for them limits, which will apply on daily CP and CNP payments and cash withdrawals at ATM machines. The limits can be set and changed at bank's branch, in online banking or in OP bank's mobile app. (OP Financial Group 2017a.)

OP bank does not offer SMS payment alerts to its clients, but the available alternative is an app called Pivo. With the use of the app clients are able to check their current balance on account and available credit, see their spendings and receive notification on payment transactions. (OP Financial Group 2017f.) It is a very convenient tool for customers to be in a full control of their current balance and be aware of transactions done from their cards. However, for fraud preventive measures SMS notification as a payment transaction alert

would still be more effective. SMS alerts are commonly being sent by banks automatically to phone numbers, which all clients have provided when applying for a payment card. In contrary, the app will not be downloaded by all cardholders and it will also require availability of internet to use it. As a result, the amount of reached cardholders by SMS alert would be higher than amount of reached cardholders by app notification. As higher is the number of cardholders, who have been reached with a payment alert, as higher is the possibility that cardholders will notice unauthorised transactions and take an action. That is why SMS alert would be considered as a more effective fraud mitigation measure.

7.2 Nordea Bank

Nordea Bank is a leading Nordic bank with representation in European countries, where it is considered as one of the biggest banks. Nordea bank's branches and representative offices can be found in the following countries: Nordic countries (Finland, Sweden, Denmark, Norway), Europe (Germany, Estonia, Latvia, Lithuania, Poland, Luxembourg, United Kingdom, Switzerland, Russia), Americas (Brazil and U.S.A.) and in Asia (China and Singapore). (Nordea 2017f.) Nordea serves private customers, small, medium and large corporate organisations (Nordea 2017d). Nordea bank's financial results in 2016 were the following: total assets of 287 bilion US dollars and net profit of 1,158 million US dollars (Corporate Finance Institute 2017).

Nordea's website www.nordea.fi has been used for the data collection and analysis. It was identified that both Visa and MasterCard payment cards with EMV chips are being issued by the bank (Nordea 2017b). A separate page on safe use of payment cards can been found under "Cards" section, where cardholders can learn about card fraud preventative services available for them. The section has been found to be very informative, but it could stand out more in order for the reader to navigate to the page easier, because right now it is located in the bottom of the "Cards" page.

First fraud preventative service, which is suggested to use when making online payments is 3D Secure feature with both Visa and MasterCard cards. Further is found information on security limits, which could be set as restrictions for daily payment volumes and cash withdrawals that are done from cardholder's bank account or credit account. Daily cash withdrawal limit in Nordea can vary between 0 € to 10,000 € and daily payments' limits are between 0 € and 50,000 €. The same limits that have been set by cardholder will apply on all transactions in different location – local in Finland or abroad. (Nordea 2017e.)

For protection against unauthorised transactions abroad Nordea offers service of geo-blocking. Nordea's clients have a possibility to authorise use of their card only in certain geographical areas. There are four options for country limitations:

- Finland
- Estonia and the Nordic countries: Finland, Sweden, Denmark, Norway and Iceland
- Europe (countries shown in table 3)
- The whole world (Nordea 2017e.)

Table 3. Countries included in "Europe" geo-blocking limitation in Nordea (Nordea 2017e)

Finland	Andorra	Italy	Monaco
Sweden	Austria	Latvia	Netherlands
Ireland	Belgium	Liechtenstein	Poland
Hungary	Bulgaria	Lithuania	Portugal
Iceland	Croatia	Luxembourg	Romania
Estonia	Cyprus	Malta	San Marino
Switzerland	Czech Republic	France	Slovakia
Greece	Turkey	Germany	Slovenia
Holy See (Vatican City)	Norway (incl. Bear Island)	Spain (incl. Canary Islands)	Denmark (incl. Faroe Islands and Greenland)
			United Kingdom (incl. Channel Islands, Gibraltar and Isle of Man)

The limits of geo-blocking service will only apply on CP payments and ATM withdrawals, but not on online purchases. Online payments can be blocked separately. (Nordea 2017e.)

All the above-mentioned services can be selected by cardholders in online banking of Nordea (Netbank), by calling customer service or visiting the banks' branch. The set limits can be adjusted any time with the use of the same channels. (Nordea 2017e.)

Furthermore, payment alerts for Nordea customers are being sent through a mobile application Nordea Pay. The application has very similar characteristics as OP bank's application Pivo. Cardholders can view their current balance, track spending and receive immediate notifications about payment transactions. (Apple Inc 2017b.) Nordea does not have SMS alert service for all cards, but only exclusively for MasterCard Credit and Gold. The alerts are being sent as SMS notifications, which will contain information on the purchase and will ask cardholder to confirm the payment transaction. In case of

unauthorised transaction cardholder can reject the payment and block the card simultaneously. The service does not need to be enabled, but starts working automatically when client receives a payment card. The phone number, which was provided to the bank will be used, thus in case if cardholder changes phone number he or she should inform Nordea about it. (Nordea 2017c.) Such service appears to be a very effective tool to spot the misuse of card immediately and prevent fraudulent payments. Offering similar service for other payment cards would definitely benefit Nordea's clients.

For Apple gadgets users Nordea now offers a newly released mobile payment application Apple Pay, which allows to make contactless payments in shop with a use of Apple smartphone. As studied earlier the application involves use of tokenisation technology for card fraud prevention purposes: the card details will not be stored on cardholder's smartphone, on Apple servers nor will be transferred to merchant during the payment. Instead the used device will be assigned a unique number and randomly generated tokens will be used for payment transactions. Payments can be done only from a device, which was connected. Additionally, for payer authentication Apple Pay is using biometrics. Cardholders are authorising payments done on the mobile device by leaving a finger print on the screen. (Nordea 2017a.) Nordea bank was the first bank in Finland that has enabled use of Apple Pay application for their customers. It can be expected that Apple Pay and similar payment applications will become more popular in Nordic countries since such contactless payment method has advantages for cardholders' use. It is convenient and quick to make a payment, which does not have a limit like a contactless card payment with a limit of twenty-five euros per purchase. (Helsingin Sanomat 2017.)

7.3 Danske Bank

Danske Bank is a Nordic bank, which has been operating for over 145 years. It serves private clients, small and medium sized businesses and institutional customers. Private customers are being served in Finland, Denmark, Norway, Sweden and Northern Ireland. (Danske Bank A/S 2017.) In 2016 Finnish subsidiary of Danske bank showed 39 billion US dollars in assets and 236 million US dollars as a net profit (Corporate Finance Institute 2017).

Danske bank's website has been used to collect data on card fraud preventative services available for its clients. According to the website Danske banks issues only MasterCard payment cards: debit and credit cards with EMV chip. (Danske Bank Group 2017b.) For protection of the cards in e-commerce environment Danske bank provides 3D Secure service for all card types. 3D Secure authentication for Danske customers has two factor

level: 1) cardholder will receive SMS to his phone with 2) a 6-digit one-time code. (Danske Bank Group 2017d.) The fact that the code is delivered to client's phone number makes the authentication more reliable meaning and diminishes fraud opportunity. This feature of the 3D secure service is an additional benefit for security of Danske bank customers' funds.

Further Danske bank offers service of identity check for MasterCard users (Danske Bank Group 2017d). MasterCard Identity Check is a new fraud preventative service, which involves use of biometrics for authentication of cardholder during online payment transaction. Instead of using codes like in 3D Secure service, cardholder will be providing a finger print or an instant photo of himself. (MasterCard 2017.) MasterCard Identity Check service is definitely supporting a more secure online payment for cardholders as well as providing stronger protection against fraud for merchants than 3D secure authentication method. The reason is that it is still possible to steal private codes, which cardholders are using for 3D secure, while biometrics are not possible to forge. Danske bank is one of the first to implement this innovative service for its customers among the benchmarked banks.

Geo-blocking service is available for all Danske bank customers and for all card types. Cardholders are able restrict and change card usage area at any time in personal online banking, by calling to customer service or at a physical bank branch. Additionally, Danske bank gives a possibility to allow usage of payment card in certain areas only on a limited time. It is a very convenient option for travel purposes. If cardholder knows exact dates of his return to a regular card usage area, he can then set a date when the geo-blocking settings should go back to old settings and block the area, where the cardholder travelled. (Danske Bank Group 2017f.) This a good addition to the service, because this way customer will not need to remember to change geo-blocking settings once more and can avoid possible fraud from occurrence.

Danske bank does not offer payment transactions alert services to its clients. One scenario mentioned on the website when bank can send SMS or make a call to cardholder to verify payment transaction is a bank transfer done to abroad. In that situation, an extra security check applies and bank will choose random international transfers and contact cardholder before making an authorization. (Danske Bank Plc 2017a.) In the UK Danske bank offers five types of SMS services. Cardholder will get notified if:

1. Balance went above the set amount
2. Balance went below the set amount
3. Balance on set day of a month
4. Debit is above the set amount
5. Credit is above the set amount (Danske Bank Group 2017c.)

This type of SMS notifications is not directly targeting fraud prevention, but mainly helping cardholders to keep track of their current balance. However, since Danske bank does not have an option of setting limits for daily payments, it could be beneficial to receive a notification if balance goes below certain level in a situation if account's funds are being exhausted by a fraudster.

On a bright side Danske bank has already added Apply Pay to its services on territory of the UK. It is expected that Apple Pay application is on the way for Danske customers in Nordics as well. The use of tokenisation and biometrics technologies will improve security of payment cards as card data will not be exposed and cardholders' authentication will become stronger. However, Danske bank has limits on the payment done with Apple Pay. The payments can't exceed 30 GBP in physical stores and online and could definitely be seen as a disadvantage from customer's point of view. (Danske Bank Group 2017a.) This is very different from Nordea's Apple Pay transactions, which do not have limits as was discussed in the previous subchapter.

Moreover, biometrics technologies are also being used in Danske mobile banking for users of Apple gadgets. Cardholders can log-in in the banking application by scanning their fingerprint on the screen of IPhone. (Danske Bank Plc 2017b.) This adds an extra protection layer and prevents fraudulent transactions in mobile banking.

8 Results

In this chapter, all the collected information from the case banks' websites will be reviewed and the card fraud prevention services will be compared against studied theory. The findings of the analysis have been summarised in Table 4, which is based on the theoretical chapter 5 "Card Fraud Prevention". Card fraud prevention services and methods that have been studied in that chapter were used as a guide to search the information and compare the banks' card fraud prevention services.

Table 4. Comparative analysis of the banks' card fraud prevention services

	OP	**Nordea**	**Danske**
EMV chip	X	X	X
Geo-blocking		X	X
Security limits	X	X	
Alerts	X	X	
3D Secure	X	X	X
Tokenisation		X	X
Biometrics		X	X
Device tracking			

Debit and credit payment cards that are being issued by OP, Nordea and Danske banks have been compared and analysed. The banks are issuing only EMV complaint cards with embedded chips as required in European Union zone. It means that the banks are providing the necessary protection against card data skimming at physical POS. However, the cards are still manufactured with magnetic stripes. As discussed already earlier in chapter 5, this happens due to the fact that not all payment terminals and POS have migrated towards using EMV technology outside of Europe. (European Central Bank 2014, 39.) Card fraud associated with this problem should be addressed outside of Europe by adopting EMV standards for all POS. Global migration to EMV technology will be a solution against card data skimming and card cloning. Meanwhile, as mentioned in Europol's report "Payment Card Fraud in the European Union" limiting geographical locations, where payment card can work, will provide a temporarily protection against fraudulent transactions done in non-EMV complaint regions. Such method is called geo-blocking and must be provided by issuing banks.

Geo-blocking service has been looked at next. Nordea and Danske banks are providing this service: cardholders can block geographical locations, which are outside of normal payment card usage area. Their clients can easily unblock the areas in case of travelling to other countries and then revert to the initial limitations settings once they are returned to country of residence. This is certainly an effective service to prevent card fraud that can occur overseas, especially taking into consideration the fact that counterfeit payment cards can be easily used in non-EMV complaint areas. For that reason, OP bank is strongly recommended to adopt geo-blocking service to provide a better card fraud protection to their clients.

Device tracking service, which involves identification of geographical location of cardholder's mobile device during payment transaction, can be called a "smart version of geo-blocking". This technique is more advanced, because it first checks location of a cardholder by tracking his/her mobile gadget, and then if the location differs from point where the payment is initiated it will block the transaction. Such advanced card fraud prevention service must be introduced as an option to cardholders, because none of the analysed banks are currently offering the device tracking in any form.

Security limits on daily CP and CNP payments as well as on cash withdrawals at ATM machines are currently offered at OP and Nordea banks. This measure has a big importance for the financial institutions. It does not directly prevent card fraud from occurrence, but it minimises potential losses associated with card fraud. For example, if cardholder sets a limit of 100€ for online payments in 24 hours, it means that even if

fraudster has stolen card data and managed to process an unauthorised transaction, he will not be able to misuse more than 100€. At this point it is very crucial for cardholder to notice the unauthorised transaction in order to prevent the following ones in the next 24hr. A suitable service for this purpose is alert service, which must be offered by banks.

Alert service is also available in the OP and Nordea banks only. The banks have a banking mobile application, which has several functions. One of them is an alert feature that allows cardholders to receive instant notifications about payments done from a payment card. Such service is aiming to inform client about potential misuse of a payment card in time. As sooner the card fraud is noticed as sooner action can be taken to prevent following unauthorised transactions. As discussed in the previous chapter alert service provided via SMS could be more effective for fraud preventative measures, since it would reach a greater number of clients. Cardholders, who might not be using banks' mobile applications should be taken into consideration and banks could offer SMS alert service as an option.

3D secure authentication for purchases in e-commerce environment is provided by all three banks. However, it is important to understand that not all online stores have integrated the 3D secure authentication. Therefore, on the websites, which do not have additional fraud prevention tool like 3D secure, stolen card data can still be misused. It can be seen that 3D secure is not an ultimate fraud prevention in e-commerce environment and it is mainly protecting merchants against fraud, but not cardholders. Banks should be offering additional and more convenient authentication services like MasterCard's Identity Check, which is provided in Danske bank. Identity Check involves use of biometrics: fingerprint scanning, facial recognition. Use of biometrics in authentication process is a next step in fraud mitigation. According to research done by Visa in several European countries cardholders are ready to use biometrics in payments. Over 70% of respondents think that payment authorisation, which involves two-factor authentication: 1) providing PIN code and 2) using biometrics technology, will be a secure option. (Visa Europe 2016). Banks should be working towards integrating authentication with biometrics for all e-commerce payments to provide up-to-date card fraud prevention methods.

According to Visa's "Annual Digital Payments" study 77% of Europeans have integrated use of mobile devices for banking and for making payments into their everyday life (Visa Europe 2017b). Based on this trend towards using mobile devices for payments it can be expected that in the upcoming years even more people will be making payments at physical shops with their gadgets instead of regular payment cards. Thus, it is very important that more payment solutions and fraud preventative measures must be provided for mobile payments. Tokenisation technology is one of the fraud prevention methods for mobile payments at

POS as well as for CNP transactions. When initiating a transaction cardholder will provide a randomly generated token instead of card information, thus card data theft will be prevented (Visa Europe 2015). Nordea and Danske banks have already integrated a payment method Apple Pay, which is based on tokenisation technology.

There are other similar payment solutions like Apple Pay, for example Android Pay. This type of mobile applications are all based on tokenisation technology to prevent card data theft. Furthermore, they have an integrated authentication solution, which is based on biometrics. Payers are able to authorise transactions with a use of fingerprint, which makes payment transactions even more secure. (Apple Inc 2017a; Android 2017.) These new technologies can be argued to be currently the best card fraud prevention methods on the market. Tokenisation technique and authentication based on biometrics must be available for cardholders to respond to current fraud mitigation trends in the industry. Additionally, Danske bank has integrated use of biometrics in online banking. This indicates that the Danske and Nordea banks are trying to adopt the newest fraud prevention tools and offer up-to-date payment solutions to their clients. It is recommended for OP bank to start offering similar payment applications, which provide tokenisation service and biometrics authentication, to their clients as well in order to respond to current card fraud challenges in CP and CNP environments.

8.1 Conclusion

After performing the comparative analysis on the card fraud prevention services of the case banks a number of conclusions have been drawn and the following suggestions and recommendations were given to the banks.

Firstly, it was found that OP bank is currently providing only four card fraud prevention services and features to its clients. It is suggested that the bank would benefit from extending the provided card fraud mitigation services by adopting the following technologies that have been already been proven effective for card fraud mitigation in other financial institutions: geo-blocking, device tracking, tokenisation and biometrics.

Secondly, following from the analysis it can be concluded that Nordea bank is currently providing a relatively wide selection of card fraud prevention services for its clients. When comparing its services to the studied card fraud prevention methods in chapter 5, it was found that Nordea is only lacking an option of providing device tracking service. Because this service provides payment authorisation based on cardholder’s device location it can be stated that it responds to a current trend of people using gadgets on daily basis and it

ensures an additional security layer for payment transactions. Thus, it would be recommended to adopt device tracking service in Nordea and other case banks, because it is not available in any of the analysed institutions.

Furthermore, OP and Nordea banks are advised to review the importance of alert service for payment transactions. Currently this service is available for banks' mobile applications users only. However, other cardholders must be taken into consideration by offering an option of SMS alerts. Alerts on payment transactions via SMS would reach more cardholders and ensure that more unauthorised transactions are spotted on time.

Lastly, it was identified that Danske bank has five card fraud prevention services from the list. While the bank is offering more advanced services like geo-blocking and tokenisation together with biometrics, it is not providing very basic fraud mitigation measures like security limits on daily payments and payment alerts for their customers. Danske bank is strongly recommended to integrate these techniques to ensure a stronger protection against fraud.

In conclusion, to ensure secure card payments to its clients banks should promptly react to arising card fraud trends by adopting up-to-date card fraud mitigation methods and monitor the card fraud market. Furthermore, it is equally important to take an active role in promoting the existing card fraud prevention services to cardholders. It can be done, for example, in face-to-face meetings with the clients and by creating a separate section dedicated to safety of payment cards on bank's website. Making sure that clients are aware of the options on how they can protect their payment cards against fraud will play a significant role in card fraud mitigation.

9 Reflections on the thesis

This is the final chapter, which includes discussion of the thesis results, my personal learning from the conducted study and ideas for further research on the topic.

9.1 Discussion of thesis results

The thesis has answered to the questions posed in the very beginning: how can card fraud occur when payment card is not physically stolen and how can banks help their clients to prevent such fraudulent transactions?

The theoretical study has identified that CNP fraud includes two phases: theft of card details and online payment fraud. Identity theft is a key part of CNP fraud process and can occur in many different scenarios, but nowadays fraudsters tend to use internet as a primary tool for such manipulations. The reason is that it is an easy and safe environment for committing identity theft. Additionally, a number of the most common identity theft techniques in card fraud were identified and discussed.

Next, with the use of latest statistics it was determined that CNP frauds constitute the biggest part of all payment card frauds. In the last years CNP fraud in Finland has accounted for 58% and 66% in Europe. The figures showed that CNP fraud is a growing concern in payment card industry and has to be addressed by all parties. Thus, card fraud prevention methods that are available in financial institutions in Europe were examined next.

To summarise, the theoretical study provided a broad overview on CNP fraud and its components. The results are considered to be reliable, because I used a combination of theoretical books and latest articles on the topic as a primary source of data for the theoretical study. The goal was to provide timely and accurate information for the research.

The research part of the thesis was focused on the application of the studied theory in real life. Precisely, a case study analysed card fraud prevention services that are currently offered in three Finnish and Nordic banks: OP bank, Nordea bank and Danske bank. The services were compared against the card fraud prevention methods studied in theoretical part. Results of the research showed that even with the variety of fraud prevention techniques available in Europe, the case banks, which are considered to be the top banking organisations in Finland, still do not offer all the available card fraud prevention services to their clients. The topic can be investigated deeper to understand particular reasons behind the findings of the research.

9.2 Own professional development and learning

Writing the thesis for me was a great learning experience. I have gained knowledge on payment card industry, how card payment process works, what are the current card fraud threats and what are the fraud mitigation methods available nowadays. This study will not only benefit for me as a cardholder, but also it will give me advantage in my current profession as I am closely working with a payment administration team and payment service providers on daily basis. Dealing with card fraud and chargebacks is a part of our online business. That is why better understanding of payment processes and card fraud will aid me in solving issues at work.

Since the studied topic was of a great interest to me and it contributed to my learning process. I was eager to find and study all the material related to the research. However, with the plenty of information available on card fraud topic it was challenging to stay on the track and not to get distracted by other interesting themes. Part of the process was constantly checking and filtering data, which is applicable to the study and which is not.

Another valuable lesson for me during the thesis writing process was time management. The planning process of my thesis took place in Spring 2016, however I was able to start the writing process itself only in the spring of 2017. The study was finalised in Autumn 2017.

9.3 Ideas for further research

Card fraud and its prevention is a versatile subject, which can be studied from different points of view. In this research, the topic has been viewed from perspective of cardholders. It was examined how do banks help clients to protect their payment cards and personal funds from fraudsters' attacks. However, the same problem could be studied from merchants' perspective. From my own working experience, I know that payment fraud is a growing concern for online businesses since losses from CNP fraud are usually being pushed to merchants. Such research would help to answer the following questions. How can merchants protect themselves from fraudulent orders and payment transactions, which end up as chargebacks and can be very damaging for a business? What fraud prevention tools can an online store implement to provide a strong cardholder authentication during a purchase? What security measures will ensure secure payment environment for a business, but will not affect customer experience in a negative way? In my opinion this would be an equally interesting research to conduct, which would bring valuable results for online businesses.

References

Albrecht, W., S., Albrecht, O., C., Albrecht, C., C. & Zimbelman, F., M. 2011a. Fraud Examination. 4th ed. Cengage Learning. Boston.

Albrecht, C., Albrecht, C. & Tzafrir, S. 2011b. How to protect and minimize consumer risk to identity theft. Journal of Financial Crime. Vol. 18. Issue 4. pp.405-414. Emerald Group Publishing Limited.URL: https://doi.org/10.1108/13590791111173722. Accessed: 10 November 2017.

Android. 2017. Android Pay. URL: https://www.android.com/pay/. Accessed: 24 October 2017.

Apple Inc. 2017a. Apple Pay. URL: https://www.apple.com/apple-pay/. Accessed: 24 October 2017.

Apple Inc. 2017b. Nordea Pay. URL: https://itunes.apple.com/fi/app/nordea-pay-finland/id1214232887. Accessed: 24 October 2017.

Bank of Finland. 2016. Payments statistics for 2014. URL: https://www.suomenpankki.fi/en/Statistics/payments-statistics/tables/. Accessed: 26 September 2017.

Capgemini. 2012. Credit Card Transaction Fraud and Mitigation Trends. URL: https://www.capgemini.com/wp-content/uploads/2017/07/Credit_Card_Transaction_Fraud_and_Mitigation_Trends.pdf. Accessed: 12 September 2017.

Card Not Present. 2015. Back to the Basics: A CNP Payments and Fraud Primer. URL: https://cardnotpresent.com/back-to-the-basics-a-cnp-payments-and-fraud-primer/. Accessed: 29 July 2017

Communications of the ACM. 2014. Inside Risks. EMV: Why Payment Systems Fail. URL: https://m.cacm.acm.org/magazines/2014/6/175170-emv/fulltext?mobile=true. Accessed: 28 September 2017.

Corporate Finance Institute. 2017. Top Banks in Finland. URL: https://corporatefinanceinstitute.com/resources/careers/companies/top-banks-in-finland/. Accessed: 24 October 2017.

Credit Card Insider. 2017. Credit Card Issuers and Networks – What's the Difference? URL: https://www.creditcardinsider.com/learn/issuers-networks/. Accessed: 7 November 2017.

Danske Bank A/S 2017. A strong Nordic bank. URL: https://danskebank.com/about-us. Accessed: 18 October 2017.

Danske Bank Group. 2017a. Apple Pay. URL http://danskebank.co.uk/en-gb/Personal/ways-to-bank/Pages/apple-pay.aspx. Accessed: 18 October 2017.

Danske Bank Group. 2017b. Products. URL: https://www.danskebank.co.uk/en-gb/Personal/Day-to-day/cards/products/Pages/products.aspx. Accessed: 18 October 2017.

Danske Bank Group. 2017c. SMS services. http://danskebank.co.uk/en-gb/Personal/ways-to-bank/Pages/SMS-services.aspx. Accessed: 18 October 2017.

Danske Bank Group. 2017d. 3DSecure. URL: https://www.danskebank.co.uk/en-gb/Personal/Day-to-day/cards/Secure-Online-Shopping/Pages/danske-3d-secure.aspx. Accessed: 18 October 2017.

Danske Bank Group. 2017e. Apple Pay. URL: http://danskebank.co.uk/en-gb/Personal/ways-to-bank/Pages/apple-pay.aspx. Accessed: 16 October 2107.

Danske Bank Group. 2017f. Geoblocking. URL: https://www.danskebank.co.uk/en-gb/Personal/Day-to-day/cards/tipsInformation/Pages/Geo-Blocking.aspx. Accessed: 3 October 2017.

Danske Bank Plc. 2017a. Extra security check. URL:https://www.danskebank.fi/en-fi/Personal/daily-banking/Pages/Extrasecuritycheck.aspx. Accessed: 16 October 2107.

Danske Bank Plc. 2017b. Voit kirjautua sisään Mobiilipankkiin sormen hipaisulla. URL: https://danskebank.fi/sinulle/tyokalut/digitaaliset-palvelut#/sormenjalki. Accessed: 18 October 2017.

DFI. 2015. ATM Skimming Devices Popping Up Across the Country. URL: http://www.dfi.wa.gov/consumer/alerts/atm-skimming-devices-popping-across-country. Accessed: 23 September 2017.

EMV Migration Forum. 2016. Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud. URL: http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/. Accessed: 7 November 2017.

Ecommerce Foundation. 2017. European Ecommerce Report 2017.URL: http://www.ecommercefoundation.org/download-free-reports. Accessed: 3 September 2017.

European Central Bank. 2014. Card Payments in Europe – a Renewed Focus on SEPA for Cards. Germany. URL: https://www.ecb.europa.eu/pub/pdf/other/cardpaymineu_renfoconsepaforcards201404en.pdf?cca00bd3ff6ef67458ef0d94a1d52518. Accessed 28 September 2017.

European Central Bank. 2015. Fourth report on card fraud. Germany. URL: https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf. Accessed: 25 September 2017.

Europol. 2012. Payment Card Fraud in the European Union. URL: https://www.europol.europa.eu/publications-documents/situation-report-payment-card-fraud-in-european-union. Accessed: 28 September 2017.

Europol. 2016. Internet Organised Crime Threat Assessment (IOCTA 2016). URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016. Accessed: 22 September 2017.

Get Elastic Ecommerce Blog. 2017. Who Needs 3D Secure? Verified By Visa and MasterCard SecureCode Examined. URL: http://www.getelastic.com/who-needs-3d-secure-verified-by-visa-and-mastercard-securecode-examined/. Accessed: 30 September 2017.

Gottschalk, P. 2010a. Categories of financial crime. Journal of Financial Crime. Vol. 17. Issue 4. pp.441-458. Emerald Group Publishing Limited. URL: https://doi.org/10.1108/13590791011082797. Accessed: 7 November 2017.

Gottschalk, P. 2010b. Policing Cyber Crime. 1st ed. Bookboon.com.

Gottschalk, P. 2016. Investigation and Prevention of Financial Crime: Knowledge Management, Intelligence Strategy and Executive Leadership. Routledge. Abingdon. New York.

Helsingin Sanomat. 2017. Apple Pay tuli Suomeen – alkaako puhelimella maksaminen nyt yleistyä? URL: https://www.hs.fi/talous/art-2000005420734.html. Accessed: 24 October 2017.

Laudon, K. C., & Laudon, J. P. 2015. Essentials of management information systems. 11th ed. Pearson Education Limited. Harlow. URL: https://ezproxy.haaga-helia.fi:2169/readonline/9781292075013. Accessed: 7 November 2017.

Laudon, K. C., & Traver, C. G. 2017. E-commerce 2016: business, technology, society. 12th ed. Pearson Education Limited. Harlow.

MasterCard. 2007. The anatomy of a transaction. URL:https://www.mastercard.com/us/company/en/docs/TheAnatomyOfATransaction.2007.pdf. Accessed: 29 July 2017.

MasterCard. 2017. Mastercard Identity Check: Mastercard makes fingerprint and 'selfie' payment technology a reality. URL: https://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/. Accessed: 18 October 2017.

Montague, D. 2010. Essentials of Online payment Security and Fraud Prevention. 1st ed. John Wiley & Sons Inc. Hoboken.

Nasdaq. 2017. How Biometrics Will Impact Payments. URL: http://www.nasdaq.com/article/how-biometrics-will-impact-payments-cm820046. Accessed: 24 October 2017.

Nordea. 2017a. Apple Pay. URL: https://www.nordea.fi/en/personal-customers/everyday-finances/cards/apple-pay.html#tab=How-to-pay. Accessed: 24 October 2017.

Nordea. 2017b. Compare cards. URL: https://www.nordea.fi/en/personal-customers/everyday-finances/cards/compare-cards.html. Accessed: 24 October 2017.

Nordea. 2017c. Nordea MasterCard SMS service. URL: https://www.nordea.fi/en/personal-customers/everyday-finances/cards/nordea-mastercard-sms-service.html. Accessed: 17 October 2017.

Nordea. 2017d. Our organisation. URL: https://www.nordea.com/en/about-nordea/who-we-are/our-organisation/. Accessed: 16 October 2107.

Nordea. 2017e. Safe use of cards. URL: https://www.nordea.fi/en/personal-customers/everyday-finances/cards/safe-use-of-cards.html. Accessed: 16 October 2107.

Nordea. 2017f. Where we operate. URL: https://www.nordea.com/en/about-nordea/where-we-are/Where-we-operate/. Accessed: 16 October 2107.

Økokrim. 2008. Annual Report 2008. Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime. Oslo. URL: http://www.okokrim.no/www/okokrim/resource.nsf/files/wwww93scs7-okokrim_annualreport_2008/$FILE/okokrim_annualreport_2008.pdf. Accessed: 8 March 2017.

OP Financial Group. 2017a. Cards. https://uusi.op.fi/private-customers/daily-banking/cards. Accessed: 19 October 2017.

OP Financial Group. 2017b. Criminals are not on summer holiday. URL: https://uusi.op.fi/-/rikolliset-eivat-lomaile-kesalla. Accessed: 20 September 2017.

OP Financial Group. 2017c. Fraudsters are phishing for online bank user identifiers and card details. URL: https://uusi.op.fi/-/huijarit-kalastelevat-verkkopankkitunnuksia-ja-korttitietoja. Accessed: 7 October 2017.

OP Financial Group. 2017d. Information on the member banks' and Helsinki OP Bank's operations. URL: https://www.op.fi/op/op-financial-group/op-financial-group/op-financial-group-member-banks?id=81210&srcpl=8&kielikoodi=en. Accessed: 19 October 2017.

OP Financial Group. 2017e. OP customers’ credentials are being requested on the phishing website. URL: https://uusi.op.fi/-/opn-asiakkaiden-tunnuksia-kalastellaan-huijaussivustolla. Accessed: 7 October 2017.

OP Financial Group. 2017f. Pivo. URL: https://uusi.op.fi/use-of-op-eservices/pivo. Accessed: 19 October 2017.

PaymentsCM LLP.2015. Payment Card Tokenization. URL: http://www.paymentscardsandmobile.com/payment-card-tokenization/#prettyPhoto. Accessed: 3 October 2017.

Pickett, S. K. H. & Pickett, J. M. 2002. Financial Crime Investigation and Control. John Wiley & Sons Inc. New York.

Radu, C. 2003. Implementing Electronic Card Payment Systems. Artech House. Norwood. URL: https://ebookcentral.proquest.com/lib/haaga/reader.action?docID=227605.

Shipley, T. G. & Bowker, A. 2014. Investigating Internet Crimes. An Introduction to Solving Crimes in Cyberspace. 1st ed. Elsevier Science. Waltham. URL: https://ebookcentral.proquest.com/lib/haaga/reader.action?docID=1115158. Accessed: 9 November 2017.

Statista. 2017a. Average annual spending per capita for online shopping in Europe in 2015 and 2016, by country (in euros). URL: https://ezproxy.haaga-helia.fi:2130/statistics/435928/online-shopping-e-commerce-spending-per-capita-by-country-europe/. Accessed: 3 September 2017.

Statista. 2017b. E-commerce payment volume index growth in Finland from 2014 to 2016. URL: https://ezproxy.haaga-helia.fi:2130/statistics/691976/finland-annual-e-commerce-payment-volume-growth/. Access: 3 September 2017.

Statista. 2017c. Most popular payment methods for online purchases in the Nordic countries in 2016. URL: https://ezproxy.haaga-helia.fi:2130/statistics/434227/e-commerce-popular-payment-methods-nordic-countries/. Accessed: 3 September 2017.

Statista. 2017d. Number of digital buyers worldwide from 2014 to 2021 (in billions). URL: https://ezproxy.haaga-helia.fi:2130/statistics/251666/number-of-digital-buyers-worldwide/. Accessed: 3 September 2017.

Square Inc. 2017. Payment Tokenization Explained. URL: https://squareup.com/townsquare/what-does-tokenization-actually-mean. Accessed: 3 October 2017.

Visa Europe. 2016. European consumers ready to use biometrics for securing payments. URL: https://www.visaeurope.com/newsroom/news/european-consumers-ready-for-biometrics. Accessed: 2 November 2017.

Visa Europe. 2017a. About Apple Pay. URL: https://www.visaeurope.com/making-payments/applepay/. Accessed: 2 October 2017.

Visa Europe. 2017b. Mobile Money Takes Off as 77%of Europeans Use their Phones to Bank and Make Everyday Payments. URL: https://www.visaeurope.com/media/pdf/45377.pdf. Accessed: 2 October 2017.

Visa Europe. 2017c. Payment tokenisation service launched. URL: https://www.visaeurope.com/newsroom/news/payment-tokenisation-service-launched. Accessed: 2 October 2017.

Visa Europe. 2017d. Verified by Visa. URL: https://www.visaeurope.com/making-payments/verified-by-visa/. Accessed: 2 October 2017.

Visa. 2013. Visa E-commerce merchants' guide to Risk management. URL:https://usa.visa.com/content/dam/VCOM/download/merchants/visa-risk-management-guide-ecommerce.pdf. Accessed: 14 May 2016.

Visa. 2015. Visa Launches Mobile Location Service to Improve Card Payment Experience When Traveling. URL: http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=2016148. Accessed: 2 October 2017.

Wells, J. 2010. Internet Fraud Casebook: The World Wide Web of Deceit. 1st ed. John Wiley & Sons Inc. Hoboken. URL:https://ebookcentral.proquest.com/lib/haaga/reader.action?docID=547180. Accessed: 9 November 2017.

Yle uutiset. 2014. Cyber attack targets personnel data of VR and other Finnish companies. URL:

https://yle.fi/uutiset/osasto/news/cyber_attack_targets_personnel_data_of_vr_and_other_finnish_companies/7431867. Accessed: 29 September 2017.