MALMÖ HÖGSKOLA
FAKULTETEN FÖR
HÄLSA OCH SAMHÄLLE

CARD-NOT-PRESENT FRAUD IN FINLAND: WHO PAYS?

AN ORGANIZATIONAL ECONOMICS APPROACH

HELI VÄLITALO

Degree project in criminology
91-120 credits
Master's programme in Criminology
June 2017

Malmö University
Faculty of Health and Society
20506 Malmö

CARD-NOT-PRESENT FRAUD IN FINLAND: WHO PAYS?

AN ORGANIZATIONAL ECONOMICS APPROACH

HELI VÄLITALO

Välitalo, H. Finnish banks' crime prevention advice for card-not-present frauds. An organizational economics approach. *Degree project in Criminology 30 hp.* Malmö University: Faculty of Health and Society, Department of Criminology, 2017.

As popularity of online banking services has grown exceedingly among Finnish consumers, it has become necessary for banks to provide their customers with safety advice against the emerging threat of card-not-present fraud (CNP) in order to protect them from monetary losses. However, it is unclear how effective this advice is and how well it is filling its purpose. This study aims to fill this gap and examines the advice provided by Finnish banks in order to protect their customers from CNP-frauds by applying an economical approach to the criminological field. A multilayered approach including a literature review, a web page quality assessment and a qualitative interview was used for this purpose. Contributing to existing literature on the enabling and constraining influences within the financial industry, this study increases the understanding of why Finnish banks' are homogenously tilting the balance towards their own private interests rather than public good.

Key words: banking industry, card-not-present fraud, prevention, institutional theory, regulation theory

ACKNOWLEDGEMENTS

I would like to thank all of those who have contributed to the process of working on and completing this thesis, either direct or indirect: my co-supervisor Ellinor Wepsäläinen for support, encouragement and constructive commentary, and my supervisor Lars Korsell for helping me through the process, providing valuable comments on my work. Also, I would like to thank my interviewee at Danske Bank for his precious time and valuable input. Last but not least, I am grateful for Emmi Kovalainen for introducing me to the fascinating world of economics.

TABLE OF CONTENTS

INTRODUCTION

The term financial crime covers a wide range of generally international criminal offences, and they have a major impact on financial sectors, both on a national and international level, and generate economic losses for businesses and for private persons and the society as a whole (Interpol, n.d.). Financial crimes are often committed via Internet, and are thus closely connected to cybercrimes, i.e. misconducts in the cyber environment and wrongful use of the Internet for criminal purposes (Enoch et al., 2013). Bringing together cybercriminals from around the world, Internet has become vulnerable to cyber attacks, phishing and the use of anonymous proxies to masquerade and sniff confidential information. This makes Internet users vulnerable to various kinds of frauds and attacks that aim to retrieve money from the victim. Online banking customers are particularly suitable targets for card- not-present frauds (*CNP*), i.e. frauds committed without the physical payment card (Enoch et al., 2013).

Payment cards are considered to be the most efficient and convenient way to pay in consumer-to-business relations, and the ways of paying are constantly changing and evolving as a result of innovations in payments, and improvements and investments in banking infrastructure (Creti & Verdier, 2011). Along with online banking services consumers are using their payment cards extensively in various situations, and payment cards are becoming a more and more common payment method (Koivunen & Tuorila, 2014). The popularity of Internet and payment cards has allowed banks to change their business model by expanding their services and giving space for innovations. The growth of online transactions has given an opportunity to both banks and consumers by providing convenience and reducing time and cost (Mahdi & Rezaul, 2012). In comparison, the increase in online transactions can be seen as a challenge to traditional banking as online transactions are less secure, causing a growing need for prevention of payment card frauds in the banking sector (ibid.).

The vulnerabilities, dangers and the fast development of Internet and technology are challenges in CNP-fraud prevention, as the crime prevention in cyber environment differs greatly from the traditional prevention of crime. In Finland, the preventive measures against CNP-frauds are slow, and the lawmakers struggle with trying to regulate the constantly evolving cyber environment effectively (Institute of Criminology and Legal Policy, 2015). Likewise, the banking industry is struggling with preventing the rapidly increasing CNP-frauds, as prevention requires high levels of expertise and adopting more effective, fast and innovative preventative measures (ibid.).

Efforts in fraud prevention are dependent on banks' and their customers' responses to the liability rules (Cooter & Rubin, 1987). Determining who is responsible can be difficult in instances of card-not-present fraud in comparison to card-present (CP) frauds, i.e. frauds due to lost or stolen cards, as a bank or an online merchant does not have any means to confirm if the user physically holds the card (Dhameja et al., 2013). To prevent disagreements in liability allocation in cases of CNP-fraud it is essential for banks to develop rules to guide their customers about payment frauds. In order to prevent CNP-frauds effectively, it is essential to understand how this regulation in banking industry is likely to develop and how the development can be directed towards a safer payment card industry.

AIM AND RESEARCH QUESTIONS

The purpose of this study is to examine the available literature about CNP- frauds, and the countermeasures used by Finnish banks in order to protect their customers from this type of crime. The aim is to question how the current knowledge about the problem is used in practice in order to define an area for new research. This study aims to contribute to existing literature on the mechanisms driving institutional structuring of banks and regulation within banking industry in a Finnish context. The use of neo-institutional theory and regulation theory allows to look beyond traditional criminological perspectives, to complement already existing knowledge and provide new insights, and to understand the enabling and constraining influences and the pressures within the financial industry. Hence, the present study has the following guiding questions:

1. In what ways are the Finnish bank customers exposed to CNP-frauds?
2. What kind of advice do Finnish banks give to their customers on how to protect themselves from CNP-frauds?

In order to discuss the two aforementioned questions, a third question incorporating the theoretical approaches will be:

3. How does neo-institutional theory and regulation theory explore the relationships and the liability between Finnish banks, and between banks and their customers, in cases of CNP-fraud?

Relevance of the study

Payment card frauds in general are an under-researched topic, especially in the Finnish context (Heikkinen & Iivarinen, 2011). Although many articles have been written about CNP-frauds and the related area of identity theft, very few consider the banking industry's incentives to confront this type of crime (Segal et al., 2011). Understanding factors that impact the prevention of CNP-frauds will lead to a better long-term adaptation of the preventive measures among banks, and is therefore a timely and significant issue for the whole banking industry. This study will demonstrate the importance of effective regulation on the field of crime prevention by taking an approach that benefits both criminological and economical field. The contributions of this study would be of interest to scholars in banking industry, sociology, criminology and economics.

Delimitations

This study focuses on Finnish retail banks, i.e. consumer banks, and therefore private banks, business banks and investment banks will be excluded. Further, credit card companies and networks fall outside of the scope of this study.

The appearance, i.e. design, graphics and the general aesthetics of a web page are important factors when conducting a webpage assessment, however, these factors do not have an impact on how well a web page is serving its function in preventing CNP-frauds. Rather, it is the quality of the content and navigation of a web page that portrays how well the web page is educating its reader. Therefore, the web page quality assessment will mainly focus on quality of the content and user friendliness, i.e. the criteria that have importance for the research topic. Further, the website quality assessment will only focus on the advice banks put to their web site, excluding the advice bank customers receive through online bank

or by post, or spoken advice customers receive by physically visiting a bank office.

BACKGROUND

Card-not-present frauds: an evolving threat

Despite improvements in security enhancements and means in detecting an preventing CNP-frauds it is constituting the largest category of fraud in Europe (Europol, 2016a; Mahdi & Rezaul, 2012). In Finland, cyber security and payment card frauds are a current, however under-researched, problem (Koivunen & Tuorila, 2011). According to Statistics Finland's preliminary data, a total of 13,300 payment frauds were recorded in January to September 2016, which was 84,8 percent up from January to September 2015 (Official Statistics Finland, 2016a). The share of CNP-frauds remains unknown, which makes it a challenging topic to study.

A CNP-fraud occurs when a criminal obtains the card number, security code and expiry date. In the majority of cases, the victims are unaware of the unauthorised use of their cards, which remain in their possession. By using this confidential data the perpetrator aims to purchase products and services online (Europol, 2016a). People using credit cards fraudulently will try to raise as little suspicion as possible in order to get the maximum use of the payment card. This is because banks routinely monitor the card transactions of their customers, looking for unusual spending patterns as part of their security practices (Symantec, 2008). Suspicious activities such as consecutive purchases from more than one country may be a signal of potential fraud and the card will be suspended.

Cyber security challenges in Finland

The popularity of Internet and online banking services have been key facilitators in several media-covered CNP-frauds in Finland. One of the most known cases is from 2011, when The Finnish National Communications Security Authority informed that personal data including social security numbers, addresses, phone number and email addresses of over 16,000 Finnish people had leaked out to internet during a weekend (YLE, 2012a). During the next few weeks over 500,000 email addresses and over 120,000 passwords were published in several Internet forums. The leaked information was used for purchasing goods online, and many suffered monetary losses. The case still remains unsolved (YLE, 2015).

In 2012, customers of three Finnish banks lost money in a spying malware attack done by Eastern European hacker group. The malware was called Zeus and distributed by spam mail all around the world (Esposito & Ryan, 2010). When opening the email, the malware was installed on the computer, and when bank customers entered their online banks using the contaminated computer, the spying malware was able to steal their data. The data was used for transferring money to hackers' account, and the monetary losses were remarkable (YLE, 2015). Similar news are common, and the increasing risks has forced Finnish banks to take actions to prevent these crimes.

Like in other European countries, using Internet in daily basis is becoming more and more popular among Finnish residents (Internet World Stats, 2016; Official

Statistics Finland, 2016b). According to Official Statistics Finland, eighty-eight per cent of the Finnish population aged 16 to 89 used the Internet in 2016, 72 per cent of them is using it several times a day. Internet usage is increasing especially among older age groups: 74 per cent of persons aged 65 to 74 were using the Internet in 2016. Among Finnish citizens the Internet is most commonly used for everyday errands, communication, searching for information and following the media, such as news. In 2016, 79 per cent had used email, and 81 per cent of persons aged 16 to 89 had used online banking services in the last three months (Official Statistics Finland, 2016b).

Table 1. Internet and online banking penetration in Nordic countries

Land	Internet users (June 2016)	Internet penetration (% population)	Online banking penetration (%)
Finland	5,107,402	93 %	86 %
Sweden	9,216,226	93 %	83 %
Denmark	5,479,054	98 %	88 %
Norway	5,167,573	98 %	91 %

Source: Internet World Stats (2016), Statista (2016)

The table above displays Internet and online banking penetration in four Nordic countries in 2016 (data from Iceland was not available). Denmark and Norway were the countries with highest per cent of Internet penetration. Along with Sweden, 93 per cent of the Finnish population had access to Internet. The last section displays the online banking penetration, and as the table shows, 98 per cent of the Norwegian population access online banking sites, making Norway the country with the strongest Internet banking penetration. With 86 percent Finland made it to third place.

Darknet: a black market for stolen goods and illegal enterprises

Tor, I2P and Freenet, often referred to as 'Darknet', are anonymising peer-to-peer networks often used for the purpose of cybercrime. Darknet is an important facilitator in CNP-frauds, as forums within Darknet form a necessary communication and marketing forum for payment card abuse (Europol, 2016ab; Symantec, 2008). Credit card information (e.g. card numbers and credit card dumps) and phishing information (e.g. email addresses) are among the most advertised and sought after goods on Darknet because they can be obtained and used for fraudulent purposes relatively easy. The amount of do-it-yourself tools and instructions have increased remarkably, and anyone with internet-connection can enter the black market and buy personal data, or create and use harmful software or attack services against banks and their customers without being highly technical (Ablon et al., 2014; Symantec, 2008).

Banking industry and CNP-frauds

Despite a bank's size or level of security, if it is offering online banking services, there is no escape from the threat of CNP-fraud towards its customers. Banks are not only trying to enrich and protect their own interests, i.e. support their customers' transactions, maintain their market value and attract new customers, but also to protect their customers from the dangers of cyber environment. To protect bank customers from unwanted risks it is essential for financial institutions to educate their customers about payment frauds. One of the most common reasons for chargebacks is a fraudulent use of a payment card, so besides providing information about the dangers of Internet, it is important for banks to inform which party is responsible for handling payment fraud events. Thus, most banks have tried to reach and inform their customers about what they should and should not do to in order to protect themselves against possible payment fraud attempts. However, it is not well known how effective these messages are and how well they reach the customers (Junger, 2016). Bank customers who are aware of the dangers and their responsibilities are often able to contribute to their own security (ibid.), but unfortunately many people are missing information, and therefore are at risk for falling victim to CNP-frauds.

Efficiency in crime prevention is measured not only by the costs of resources used, but also by the public good achieved by them. Representing private businesses and being driven by consumers demand, technological improvement and business motivation (Mahdi & Rezaul, 2012), banks may behave in a way that is systematically biased to the advantage of their own interests, displacing the public good (Cooter & Rubin, 1987; Segal et al., 2011). Thus, to understand the behavior of Finnish banks and their customers in CNP-fraud prevention it is necessary to take an economical and organizational approach.

THEORETICAL FRAMEWORK

With two different paradigms it is possible to take a closer look at the relationships between banks', and relationships between banks and their customers. The first paradigm is the neo-institutional approach, which views institutions' behavior as a part of a social process influenced by institutional environment (DiMaggio & Powell, 1983). The analysis of the institutional framework has revealed that banking institutions tend more and more to look alike and become uniformed. The second paradigm is based on the two concepts of regulation theory - public interest and capture. The public interest perspective views regulation supplied in response to the demand of the public, while capture refers to regulating agencies shaping their rules to protect their interests (Stigler, 1971).

Neo-institutionalism: categorical rules conflict with the logic of efficiency

Neo-institutional theory, also known as new institutional theory, is one of the main theoretical perspectives used to understand organizational behavior. According to the neo-institutional approach, the building blocks of institutional action - actors and roles, structures and goals - are constituted as social entities by an evolving set of rationalized patterns and models (Meyer & Rowan, 1977).

Neo-institutional theory looks at the structuring and influencing in institutions, proposing that the institution's formal structure is not only a product of pressures in the market, but that it is also influenced by the institutional environment, that is, an open environment consisting of other institutions. Besides being influenced by other institutions, institutions are under the pressure throughout society via public opinion, religion and law. All of these areas are influencing each other through a continuous loop (DiMaggio & Powell, 1983). In this environment, the main goal of institutions is to survive and gain legitimacy. Practices and structures of institutions are considered as either reflections of, or responses to the rules, norms and traditions deep-rooted in the institutional environment. Variations in institutions' behavior occur due to differences in regulating pressures or interorganizational influences (Bakir, 2013; Powell, 2007). The institutional rules and norms often conflict with the logic of efficiency, meaning that as a result of the conformity institutions tend to become more similar, which is hindering institutions from becoming more efficient (DiMaggio & Powell, 1983:147; Meyer & Rowan, 1977:355). This leads to the concept of isomorphism.

Institutional isomorphism: organizations become similar to each other by following institutional rules

One of the most popular institutional views that has emerged is institutional isomorphism. According to DiMaggio and Powell (1983), institutional isomorphism occurs when people in an institution adopt and obey the rules and norms of the institutional environment. DiMaggio and Powell (1983) outlined three interacting mechanisms that institutions are impacted by, leading them to become homogenous and dependent on their environment: coercive, mimetic, and normative isomorphism.

Coercive isomorphism is the basic concept of isomorphism. It refers to the adoption of a particular institutional action or design resulting from experienced institutionalized pressure, causing the institution to act in a certain manner in order to seek legitimacy. Legitimacy refers to the perception of an institution and its actions being valid, desirable and appropriate, and it justifies who has the power and wealth needed for coordination and control of the market (DeJordy & Jones, 2008:682). Coercive isomorphism often occurs when dominant institutions force the less-dominant ones to adhere to their values, norms or institutional requirements (Thornton, 2011; Bakir, 2013). This mechanism can be seen especially in governmental and legal environments (DiMaggio, 1983).

Institutions often copy practices from successful institutions. Mimetic isomorphism occurs when institutions facing uncertain environments mimic practices they consider effective, leading to similarity (DiMaggio & Powell, 1983). DiMaggio and Powell (1983) identify uncertain environments simply as institutional environments that encourage institutions to mimic similar institutions they see as legitimate. An example of mimetic isomorphism is the pressure for a bank to offer services that other banks provide (e.g. higher security in online banking).

Sharing information often stimulates development of institutions. Differing from the two other forms of isomorphism, normative isomorphism is based on the influence of professionalism and networks. It occurs through the adoption of practices considered convenient by market, industry, and professional associations, resulting in homogenization of concepts and models (DiMaggio &

Powell, 1983). For example, professionalization in the banking industry leads to isomorphism when its members interact and share their experiences.

Regulation theory: a behavioral economics perspective

Regulations are one of core functions of states and institutions: they are essential to the proper function of economies, as they create the 'rules of the game' for the players (OECD, 2011:7). In short, regulation theory explains why rules are introduced and whom they are serving, and explores the ways in which regulators interfere for society's benefit - or harm (Hardy, 2006). Regulation is generally defined as legislation imposed by a government on individuals, but can also be seen as a financial institution's attempt to control and modify its customers' behavior. Bank customers are influenced by guidelines and rules, as well as by the information the banks are providing. This is creating a regulatory regime regarding payment card security and liability that is necessary for banks in the interest of decreasing the costs of CNP-frauds.

Traditional concepts of regulation: public interest and regulatory capture

A large body of economic theories has been amassed to help understand what an optimal regulatory regime should aim to achieve and the means through which it should operate (Wren-Lewis, 2010). Two main alternative views of the regulation are widely held (Stigler, 1971:3). The first one proposes the question: "Is the ultimate goal of regulation to pursue some conception of general good, however mean-spirited, messy and confused the process may seem at any given time?", which is known as the public interest theory of regulation (Levine & Forrence, 1990:167). The public interest theory, developed by Arthur Cecil Pigou, is a theory about what motivates regulators, as well as a theory about what should motivate them. Public interest explains, in general terms, that regulation seeks the protection and benefit of the public at large (Levine & Forrence, 1990:168-9).

Opposing the public interest perspective, the second view asks "Is regulation simply an arena in which special interests contend for the right to use power for narrow advantage?" (Levine & Forrence, 1990:167). The term regulatory capture refers to the process where regulation is designed and operated to serve regulators' interests (Hardy, 2006:3). The self-interests are usually linked with the need to strengthen and gain benefits, reputation and protection (Stigler, 1971).

METHODOLOGY

Data collection and materials

Three different data collection methods were applied in this study: literature review, semi-structured interview and web page quality assessment. These methods are considered appropriate as they complete each other, and have different strengths and weaknesses, which will be described below.

Literature review

The aim of the literature review was to find the most relevant and important work within the research topic, and to adequately describe the extracted information as well as identify central issues on the research subject. This literature review operates as a foundation for the parts two and three of the thesis.

Procedure

The literature review began with searches in several databases. In the database searches, published articles as well as reports from stakeholders dealing with CNP-frauds were included. To obtain diversity, literature from different publishers, countries and authors was selected for the review. Only published and peer-reviewed articles were selected for review in order to obtain high quality. The literature used is written in two languages, Finnish and English. The sample was limited to a time frame from year 2000 through 2016, as the aim was find as recent information as possible, since cyber environment and CNP-frauds are constantly evolving.

A total of fourteen articles and reports published between 2000 and 2016 were reviewed. The majority of the articles were published in the last five years, which shows the growing importance of the research topic. A list of the most relevant keywords was constructed, and literature was searched in databases Econlit and LubSearch with the following words: *banking industry, card-not-present fraud, cybercrime, cybersecurity, payment fraud, phishing, prevention*. As mentioned before, it was chosen to include Finnish literature in order to capture variation to the literature review. To find literature in Finnish the database TamCat from the University of Tampere was used. Searches in TamCat database were conducted by using the following words: *Internet, kyberrikollisuus (cybercrime), maksukorttipetos (payment fraud), maksukortin väärinkäyttö (fraudulent use of payment card), pankkiala (banking industry).* Not all categories were represented in all searches. When searching with key terms 'payment frauds' and 'prevention', the results provided several articles about fraudulent use of payment cards. Articles describing non-financial or non-technical identity thefts, as well as those describing only card-present frauds were excluded from the review. Also, articles about other banking than retail banking were excluded.

It was difficult to find reports published by authorities in the chosen databases. Thus, Google Scholar was used for literature search, as search results in Google Scholar contain great amounts of grey literature, i.e. articles not formally published by commercial academic publishers (Haddaway et al., 2015). Google Scholar's reliance has been greatly debated (Gehano et al., 2013; Haddaway et al., 2015), but it has been concluded to be a great tool for complementing literature searches, however, it should not be used alone (see Haddaway et al., 2015). By using Google Scholar as a supplement it was possible to find relevant reports for this literature review.

Snowball method was used as another approach to find literature. When conducting the literature search, a start set of papers was identified for the procedure. By looking at the reference lists of these articles and reports, relevant and highly cited literature in the research area was identified. Articles that did not fulfill the criteria for publication year and type of publication were excluded. When articles fulfilling the criteria were found, their abstracts were read first and then the articles were scanned through until a decision was be taken to either include or exclude them.

Web page quality assessment

Banking websites are used to convey information between the bank and its customers. Conveyed information comes in different types, languages and forms and incorporates usually text and images, sometimes videos and audio, intending to inform, advise or even change attitudes or beliefs of the web page users. The objective is to make a website useful, profitable, and easily accessible (Moustakis et al., 2004). In order to understand how banks' are trying to prevent CNP-frauds it is necessary take a closer look at the advice banks' provide on their security web pages.

A web page quality assessment is a tool for detailing and evaluating aspects related to the quality in use and content, and it is a great method for critically approaching web pages (Hasan & Abuelrub, 2011). Based on the framework by Hasan & Abuelrub (2011), this website quality assessment aims to evaluate eight Finnish bank websites' security pages. This assessment is based on the evaluator's interpretation, i.e. each evaluated aspect is a matter of subjectivity.

The eight largest retail banks operating in Finland were chosen (the name in Finnish is in parenthesis): Nordea, S-Bank (S-Pankki), Savings Bank (Säästöpankki), Danske bank, Ålandsbanken, SEB, Handelsbanken and OP Financial Group (Osuuspankki). The table below shows the basic information about these banks. Information shown in the table was found at the banks' web pages, however, some banks did not provide this information online and therefore were contacted by phone and email. The amount of Finnish customers at SEB remains unknown, as they do not register their customers based on their country. Handelsbanken was not willing to give out this information for research purposes.

As the table shows, both Finland-based and foreign banks are included in the sample. OP Financial Group, Nordea and S-Bank are the three largest banks included in this study. All banks are commercial banks, which means that they provide various services, such as accepting deposits, offering investment products and issuing loans (Investopedia, n.d.).

Table 2. Information about the banks

Bank	Private individual customers (2016)	Origin	Type
Nordea	2,8 million	national	commercial
S-Bank	2,9 million	international	commercial
Savings Bank	500,000	international	commercial
Danske Bank	1,0 million	national	commercial
Ålandsbanken	13,000	international	commercial
SEB	unknown*	national	commercial
Handelsbanken	unknown*	national	commercial
OP Financial Group	3,9 million	international	commercial

Notes. * The amount of private individual customers was not available

Assessment criteria

The website quality assessment hierarchy by Hasan & Abuelrub (2011) (see Figure 1.) was used as a starting point, and to further break down into sub-criteria in order to develop a model to evaluate the quality of the banks' web security web pages.

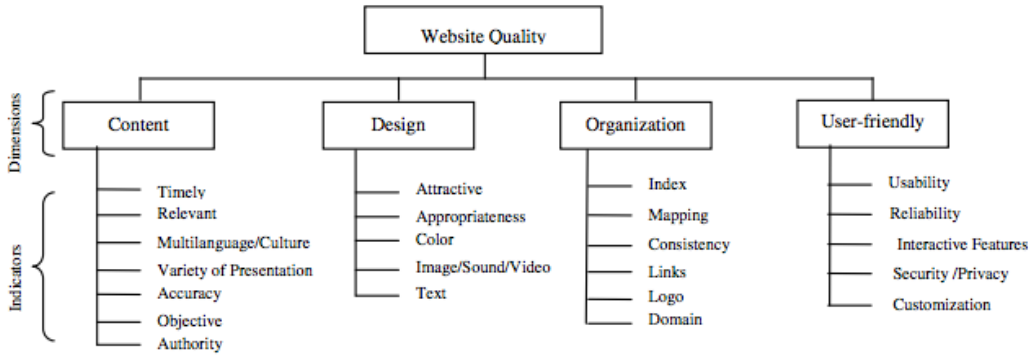

Figure 1. Website quality hierarchy by Hasan & Abuelrub (2011)

In order to build a model for evaluating banks' security web pages the four dimensions from the Hasan and Abuelrub's hierarchy were translated into three dimensions. The built model consists of following three dimensions: content, design and organization, and user-friendliness, and these are further categorized into relevant indicators (see Figure 2. below). Several indicators (e.g. authority, i.e. possible sponsors and copyright issues, and logo, i.e. the appearance of the organization's logo) were considered less important for this study therefore were excluded from the assessment.

Dimension	Indicators	Description
Content	Timely Relevant Multilanguage Variety of presentation Objectivity	Up-to-date information Comprehensive and complete information, right level of details Use of different languages Different forms (text, audio, video) Objectivity of presentation
Design and organization	Attractiveness Links	Pleasant and organized look Properly working links
User-friendliness	Usability	Easy to use, understand and navigate

Figure 2. Overview of the assessment criteria

The different indicators are rated using a 3-point scale (3=good, 2=satisfactory, 1= poor) and these are detailed below.

INDICATOR	3 = good	2 = satisfactory	1 = poor
Dimension 1: Content			
Timely	All three methods	Two methods	One or zero methods
Relevant	Complete and comprehensive	Average	Lacking and incomprehensive
Multilanguage	Two or more additional languages	One additional language	Only Finnish
Variety of presentation	Two or more additional forms of presentation	One additional form of presentation	Only in text format
Objectivity	Not biased	Might be biased	Biased
Dimension 2: Design and organization			
Attractiveness	Strong visual appearance	Like others	Unattractive
Links	All links working properly	One dead link	Several dead links
Dimension 3: User-friendliness			
Usability	Easy to use	With effort	Difficult to use

Figure 3. Rating scale for web page quality assessment

Dimension 1: Content

As the table above shows, the first dimension is content. Content refers to quality, completeness, degree of specialization and reliability of information presented on a website (Moustakis et al., 2004). To evaluate banks' security web pages, the content dimension is translated into following indicators: 1) timely, 2) relevant, 3) multilanguage, 4) variety of presentation, and 5) objectivity.

Timely evaluates the currency, i.e. whether website's information is up-to-date (Hasan & Abuelrub, 2011). Evaluating currency of the banks' web pages is particularly important since methods of CNP-fraud are evolving fast, and therefore it is expected that banks update their advice regularly. Phishing, data breaches, and malware (for definitions, see Literature review) are the most common methods used to commit CNP-fraud at the moment (Symantec, 2016), and in order to the advice be classified as 'up-to-date' banks should give information about each of these methods.

The second indicator, relevant, refers to the extent to which information is comprehensive and complete. In order to effectively educate customers the information about CNP-frauds should be thorough, high quality and provide the right level of details. Multilanguage, the third indicator, refers to the use of different languages (Hasan & Abuelrub, 2011). It is important for banks to provide advice in several languages in order to educate those who are not comfortable with reading in Finnish.

Variety of presentation relates to the different forms (e.g. audio, video) in which information is presented. Allowing the bank customer to choose a presentation form that is most appealing for him or her makes the customer more interested

and more open to the information that is provided through the security web page.

The last indicator, objectivity, refers to objective presentation of information on a web page (Hasan & Abuelrub, 2011). Objectivity of the information is highly important, as banking customers need to be offered advice that is free from cultural, religious or political biases.

Dimension 2: Design and organization

Design of a website can be critical for drawing attention of users and plays a key role in determining how long a user stays on the webpage and further explores it. Attractive, organized and easily accessible webpages will motivate users to return to it (Sutcliffe, 2002). In order to attract bank customers to read the security information, it is important that the security web page looks pleasant and feels convenient. Combining two of dimensions from Hasan and Abuelrub's model, the second dimension includes design and organization. Design consists of elements such as images, colors, videos and font, while organization refers to elements that help users to feel comfortable within web pages' layout (Hasan & Abuelrub, 2011).

From the dimensions of design and organization, the indicators of attractiveness and links are included in this assessment, as they are most relevant for how quickly bank customers will reach the required security information. Attractiveness includes use of graphic elements (e.g. photos, illustrations) that make the user satisfied when browsing the security web page (Hasan & Abuelrub, 2011). A pleasant looking security web page is likely to attract bank customers and encourage them to browse further and re-entering the page in future. The second indicator, links, relates to whether provided links on the web page are working properly. In order to help bank customers to feel comfortable and provide as comprehensive information as possible, it is necessary that links on the banks' websites are taking customers where they are intended to go.

Dimension 3: User-friendliness

The last dimension incorporates the user-friendliness of the website. This dimension concerns issues that help users, regardless of their education or experience, to find the needed information within a reasonable time. From the Hasan and Abuelrub's model, usability indicator has the most impact on how bank customers perceive and explore a security web page, and therefore no other dimensions are included in this criterion. Usability refers whether a website is easy to use, i.e. easy to understand, operate, find information, and navigate (Hasan & Abuelrub, 2011).

Qualitative interview

Due to the magnitude of the research problem there was a need to collect as much information as possible in order to be able to accomplish a deeper understanding of the research area. Thus, it was decided to use qualitative interview to collect primary data and use it to draw conclusions. The interview was conducted with a security expert within Finnish banking industry.

Recruitment and participants

One of the struggles in conducting research successfully is obtaining access to the field, especially if the topic of research is sensitive. Aiming to seek information about a topic that is beyond banks' published reports, the research topic of this

study is considered sensitive. Further, being a controlled industry, the researcher is often required to be part of the culture and speak the language of the banks in order to gain access to the field (Monahan & Fisher, 2015). Lack of this and sensitiveness of the research topic caused major difficulties in securing the cooperation with Finnish banks. Especially lack of contacts made it difficult to enter the banking industry for research purposes. Several Finnish banks and experts dealing with payment frauds and cyber security were chosen by surveying banks' websites and online publications, and then contacted by email explaining the nature of the research project. By providing information about the study to as many people as possible the aim was to generate stakeholder's interest and identify and target those who had valuable information.

However, the size and structure of banks caused problems in the recruitment process. The size of the Finnish banking industry, as well as the lack of internal communication in banks made it a challenge to obtain access to the field. For these two reasons the sampling process suffered from non-response during the recruitment. Luckily, snowball strategy was an aid to reach the hard-to-reach bank experts. A few of the identified experts were used to refer and give contact information to other stakeholders and experts who might be interested in participating in the proposed study. This made it possible to locate and contact people unknown for the researcher.

After successfully establishing contact to the field and discussing with several experts on the research area, Danske Bank volunteered to participate. The interviewee was informed about his rights and the preparation of the interview began. The interview guide was built on previous research about CNP-frauds.

Semi-structured interview

Semi-structured interview follows a checklist of themes and questions to be covered during the discussion (Bryman & Bell, 2007). The reason for choosing semi-structured interview as a method for this study was its aim to encourage the interviewee to freely discuss his own opinion on how banks advice is corresponding with the problem of CNP-frauds. The strength of a semi-structured interview is its spontaneity, in that it allows the interviewee to explore and expand his or her thoughts in depth, rather than relying on themes defined in advance of the interview (Denscombe, 2010:175). A clear list of themes is addressed during semi-structured interviews, and the interviewees are encouraged to discuss and reflect, as well as to speak widely on the emerging ideas. Therefore, the answers will be open-ended and there will be more room for discussing and expanding chosen points of interest (ibid).

Interview technique

People respond differently depending on how they perceive the person asking the questions. The interviewer needs to be polite and punctual, receptive and neutral, in order to encourage the right climate for an interviewee to feel comfortable and provide honest answers (Denscombe, 2010:182-6).

By following the guidelines by Miller-Adams and Myers (2003) it was ensured that the access to the banking field translated into information. First, it was important to be prepared by getting familiar with the organisation and have a good understanding of how the bank is going about its work in CNP-fraud prevention. Bank members may be unwilling to spend the effort to educate an amateur in the

basics of their operation, especially if this knowledge can be gained from their website's published sources. Second, learning to speak the technical language of banking industry was an important step in transforming access to information, by making it easier to understand how bank personnel approach questions they are asked to answer (Miller-Adams & Meyers, 2003:91-2).

Procedure

The interview took place at Danske Bank's office, located in northern Helsinki. The interview was recorded to ensure that nothing that is said during the interview is missed. The participant was assured anonymity and asked to give permission for the discussion to be recorded. Before starting the interview, the aim and general information about the study was described to the participant. After the interview, the audio record was transcribed as soon as possible into written text to help with the analysis of the data. Once the data was transcribed the audio files were deleted. The material is stored on a laptop by using VeraCrypt encryption software to prevent third parties to come in touch with it.

Thematic analysis: recognizing the emergent themes

The method applied to analyze the interview material is thematic analysis, and it is a qualitative analytic method for:

'identifying, analysing and reporting patterns (themes) within data. It minimally organises and describes your data set in detail. However, frequently it goes further than this, and interprets various aspects of the research topic.'

Braun & Clarke, 2006, p.79

Thematic analysis is considered to be appropriate for studies seeking to discover using interpretations, proving a systematic element to data analysis. It allows theoretical freedom, and through this allows for rich, detailed and complex description of data. It is a great tool for identifying and describing implicit and explicit ideas, giving a possibility to link the various concepts and opinions together (Namey et al., 2008).

Thematic analysis provides the opportunity to code and categorise data into ideas that are then applied or linked to raw data (Namey et al., 2008:138). An idea, i.e. a theme, captures meaningful aspects related to the topic of research and represents some level of patterned response or meaning within the data (Braun & Clarke, 2006:82). The themes become the categories for analysis.

Procedure

The transcription of the interview was orthographic, meaning that focus was on what was said during the interviews, rather than *how* something was said. After all the data had been transcribed, the whole data set was read through and a list of ideas was constructed. The analysis was done manually by using Braun and Clarke's (2006) guide' to the 6 phases of conducting thematic analysis. The six phases are: 1) Becoming familiar with the data. 2) Generating initial codes; 3) Searching for themes; 4) Reviewing themes; 5) Defining and naming themes; and 6) Producing the report.

Ethical considerations

As described previously, the interviewee received verbal and written information about the study, such as the aim with the study, methods, how the collected data

would be handled and that participation was voluntary before the interview in order to make an informed choice of whether to participate. Further, the participant was informed about that he could withdraw from the study at any time.

RESULTS

Banks and CNP-frauds: a literature review

In this section, an academic literature overview of the most common ways bank customers are exposed to CNP-frauds is presented. This literature review shortly defines the terminology associated with malicious CNP-fraud attempts against bank customers, and considers the most common means by which attacks may be delivered to customers of online banking. Finally it will examine the liability allocation in cases of CNP-fraud and the preventive measures against this type of crime.

Threats in the digital environment

Identity fraud

Identity theft is easily associated with money, as most cases involve criminals using the identity for making purchases or transactions, however, financial identity theft is only one example of the several types of identity theft that exists (for a detailed view of different types of identity theft, see Symantec, 2008:24). Identity theft occurs when a person's confidential information, such as payment card details, are wrongfully obtained. Identity fraud, however, is often but not necessarily the consequence of an identity theft, and it refers to the use of another individual's confidential information for harmful purposes, such as for economic gain. The victims of identity fraud do not only suffer monetary losses, but also several forms of psychological damage, e.g. fear and anxiety (Cassim, 2015).

Identity theft can be committed without technical means via physical ways, or with technical means by mail or online (Cassim, 2015). Methods of online identity theft include phishing, data breaches, use of malware (see chapters below) and spoofing (for definition, see Appendix 1).

Phishing

Through 2000s, phishing has developed into one of the most widespread threats in the cyber environment. Phishing refers to an attempt to trick people into disclosing confidential information by using false emails, text messages or websites designed to mislead users, and it can either be used on its own or as a preliminary step to spread harmful software or spyware (Europol, 2016a). The email addresses and phone numbers have typically been illegally stolen from hacked databases or collected from public areas on the Internet, such as social networking sites and forums. The confidential information is phished by emulating the trusted brands of well-known banks, the police, e-commerce and credit card companies (Shekokar et al., 2015; Symantec, 2008). Information such as usernames, passwords, social identification information, credit card details, bank accounts, and date of birth are the personal identity details frequently sought by phishers. Using social engineering techniques, i.e. psychological manipulation (for more detailed definition, see Appendix 1), phishers aim to compromise the receiver with interesting, even scary subject lines and content. Common subjects

include disclosed passwords, tax refunds, fake orders, lottery winnings and fake emails from banks and other financial institutions (see Appendix 2 for an example of the content in a phishing e-mail) (Enoch et al., 2013; Kessem, 2012). Phishing messages often include a URL, which directs users to a web site where they are asked to enter their confidential information. These phony web sites are built by using visual-based content such as page layouts, styles, key regions in purpose to make the false website appear and react exactly the same as the legitimate one (Enoch et al., 2013).

The amount of phishing attacks is rapidly increasing and becoming more organized. Poor drafting, weak grammar or spelling do not always indicate whether a message or website is phony, since the quality of phishing scams have improved (Europol, 2016a; Grazioli & Jarvenpaa, 2000). The extent and quality of phishing has been increasing due to the availability of phishing attack tools and kits on the underground market (Ablon et al., 2014). Thousands of professional-looking phishing websites continue to be set up daily as a result of these easily available and easy-to-use tools, and this may result in that phishing becomes more and more associated with new, less skilled cybercriminals, while more skilled cybercriminals shift their focus to targeted attacks, so called spear phishing attacks, data breaches and developing harmful software and spyware (Enoch, et al., 2013; Europol, 2016a).

Spyware and malware

Bank customers are increasingly targeted by e-mails attached with malware and spyware (Dhameja et al., 2013; Mahdi & Razoul, 2012). Spyware refers to viruses that are capable of capturing keystrokes entered into a computer keyboard in order to steal sensitive user data, while malware refers to any harmful software entering a system without user or system authorisation. Malware includes viruses, worms and Trojans (for a more detailed overview of different kinds of malware, see Symantec, 2016). As with phishing fraud, malware and spyware are not only distributed in e-mails, but also in text messages or websites, and it requires social engineering techniques in order to convince its recipient to open the attachment or to click on a link (Mahdi & Razoul, 2012; Symantec, 2016).

Data breaches

Any Internet facing sector storing confidential information, regardless of its function, needs to consider itself and its system to be a target for data breach attempts. Cybercriminals are not only interested in targeting bank customers with phishing messages and malware, but also banks which might to leak confidential information. In fact, banks are a key target of data breach attempts, as financial data is particularly sought at the black market (Europol, 2016a; Symantec, 2016).

Responsibility in fraudulent use of payment cards

Customer's liability in case of CNP-fraud

When a bank customer falls victim for phishing, malware or data breach and suffers monetary losses, it is important that the rights and responsibilities of all the parties included in the chargeback procedure to be clearly defined (Dhameja et al., 2013). The European union's *Directive 2007/64/EC on payment services in the internal market* and *Directive 2008/48/EC on credit agreements for consumers* compose the legal bases to a cardholder's liability for fraudulent use of his payment card (European Consumer Centres Network, 2014). Consumers need to

take three steps in order to resolve problems related to unauthorized use of debit or credit card. The first step is to contact the issuing bank in order to stop the unauthorized use of the card. The onus of proving whether a card transaction has been authorised by the cardholder is borne by the issuing bank.

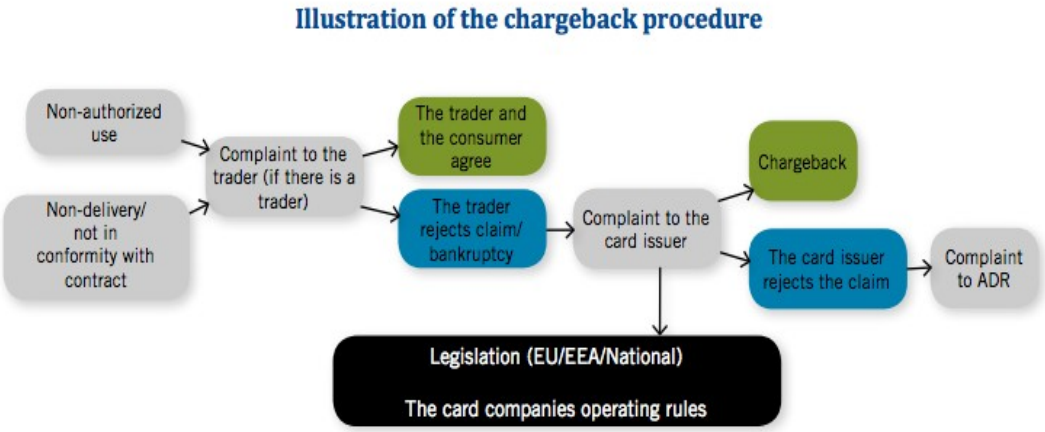

Figure 4. Illustration of the chargeback procedure (European Consumer Centres Network, 2014:5)
Notes. ADR refers to a public third-party organization dealing with consumer complaints

After the damage comes clear to the customer, the second step is to seek chargeback directly from the issuing bank (Koivunen & Tuorila, 2015:39pp). The general rule is that when a payment card has been charged without authorization from the cardholder, e.g. if the card has been stolen, the payment service provider shall refund the amount to the card holder (European Consumer Centres Network, 2014).

The cardholder is required to keep personalised security features safe and keep track of payment transactions on their account, otherwise they will risk being seen as grossly negligent and therefore refused a refund in a situation of payment fraud. In case of gross negligence the cardholder shall bear the losses relating to the unauthorised transactions, up to a maximum of 150 euros (Directive 2007/64/EC; European Consumer Centres Network, 2014). In the Zeus malware attack against Finnish bank customers in 2012 the liability allocation was determined case-by-case. In order to receive chargebacks the victim had to have secured his computer with a proper firewall (YLE, 2012b). The liability varied depending on the banking contract agreements between the bank and the cardholder, allowing banks to place their own voluntary caps on liability.

In case the bank's response is unfavourable the customer may contact a third-party organization dealing with consumer complaints. The Consumer Disputes Board (CDB) and the Banking Complaints Board (BCB) are the two Finnish equivalents of ADR that address consumers' complaints in liability issues (Koivunen & Tuorila, 2015:40). A decision reached by the organizations is a recommendation for both parties (FINE, 2016; Koivunen & Tuorila, 2015:40).

Responding to the emerging threat

Preventive measures against CNP-frauds

Consumers and financial institutions are able to reduce payment fraud losses by taking several precautions, however, these have not shown significant effect in preventing CNP-frauds. Already in 2004, researcher Kenneth Wesley posed the question: 'If the technological advances in credit card fraud detection are so significant, why then are losses not significantly reduced? '(Wesley, 2004:7). This topic is still a current issue (Koivunen & Tuorila, 2015).

Having strong passwords and changing them frequently, shredding hardcopies, a regular practice of logging off when leaving a computer and manually verifying the security of a website are examples of low tech methods that can be used in order to prevent CNP-frauds (Enoch et al. 2013; Symantec, 2016). To prevent phishing a wide range of anti-phishing programmes, such as McAfee Siteadvisor® and PWDHASH®, as well as detection techniques, have been developed. Two of the most used techniques are whitelisting and blacklisting. White lists manage a list of known-good websites, and they are generally divided into lists updated by central servers and personalized lists managed by the end users. In comparison, black lists manage a list of known-bad websites, but unfortunately this approach is only effective as the quality of the list. As thousands of new phishing websites are set up daily, many non-blacklisted phishing sites are not recognized (Enoch et al. 2013).

Furthermore, methods such as fingerprint and facial technologies are despite their high price becoming more prevalent means of CNP-fraud prevention. Other high tech methods such as fraud monitoring and credit bureau reporting are adding additional preventive measures against card frauds (Enoch et al., 2013).

Web page quality assessment

Six of the eight banks provide information and advice about CNP-frauds on their website. Two of the banks, SEB and Handelsbanken did not fill the inclusion criteria, as they did not have any security advice about payment frauds on their website when the evaluation was conducted, and for this reason are excluded from the assessment.

Results from the web page quality assessment are presented below.

BANK	CONTENT					DESIGN AND ORGANISATION		USER-FRIENDLINESS	TOTAL SCORE
	Objectivity	Multilanguage	Variety of presentation	Relevant	Timely	Attractiveness	Links	Usability	
Nordea	3	3	1	3	2	3	3	3	3
S-Bank	3	1	1	2	1	3	3	3	2
Savings Bank	3	3	1	1	1	3	3	2	2
Danske Bank	3	1	2	3	2	3	3	3	3
Alandsbanken	3	2	1	1	1	3	3	1	2
SEB	-	-	-	-	-	-	-	-	-
Handelsbanken	-	-	-	-	-	-	-	-	-
OP	3	3	2	3	2	3	2	3	3

Figure 5. Overview of the assessment results (3=good, 2=satisfactory, 1= poor)

Content

As the figure above shows, the security information of each bank is presented without political, cultural or religious biases, and each bank was evaluated as 'not biased'. Nordea, Savings Bank and OP Financial Group are the only banks offering security information in three languages (Finnish, English and Swedish). Ålandsbanken offers information in Swedish and Finnish, and other banks provide information only in Finnish. Regarding the variety of the presented information, most of the banks do not use videos or audio as a form of their presentation. As the table shows, Danske Bank and OP Financial Group scored higher in this category. To make phishing more comprehensible Danske Bank uses pictures of real-life examples of phishing messages its customers have received. OP Financial Group, in comparison, uses an instructional video to illustrate how customers use online banking services safely.

As the figure shows, the scores in the relevant category vary. Each bank gives at least basic information, i.e. how to report a fraud and how to use payment card safely. In this category, Savings Bank and Ålandsbanken are the worst with the score of 1, as they only provide the basic general information about safe payment card use, while S-Bank scores in the middle with average amount of security advice. Nordea, Danske Bank and OP Financial Group scored highest: these three banks give the most comprehensive and complete information about CNP-frauds and how bank customers can protect themselves from falling victim for CNP-fraud. Further, the security web pages by Nordea and S-Bank include a section for frequently asked questions about payment frauds.

Three banks, S-Bank, Savings Bank and Ålandsbanken, were rated the lowest in timely category. S-Bank gives information only about phishing, however, as the relevant score shows, this information is somewhat comprehensive. As in relevant category, Savings Bank and Ålandsbanken scored low in timely category. Neither of them provides information about the most common methods of CNP-fraud. Nordea, Danske Bank and OP Financial Group present two of the methods, phishing and malware. None of the banks gives information about data breaches.

The Table 3. below illustrates the topics banks' web pages covered.

Table 3. Covered topics

	Nordea	S-Bank	Savings Bank	Danske bank	Ålands Banken	OP
How to report a fraud	x	x	x	x	x	x
Safe use of payment cards	x	x	x	x	x	x
How bank contacts its customers		x		x	x	x
Malware	x			x		x
Data breaches						
Phishing	x	x		x		x
How to increase web security	x	x				x
Liability allocation	x			x		
Bank's measures to prevent CNP-frauds	x					x

Each security web page provides advice about how a customer can report a payment fraud or an attempt to fraud, as well as how customers can use payment cards and Internet safely. Each bank state that customer should not give the physical payment card or their PIN to third parties but only Nordea and Danske Bank give information about customer's liability in CNP-cases. Nordea and Savings Bank are the only banks that do not mention how they contact their customers, while other banks' state that they do not contact their customers by e-mail or phone asking their personal information. Nordea and OP Financial Group are the only banks to provide information about the preventive measures they are using in order to protect their customers from CNP-frauds. Furthermore, each bank provides a link or several links to external information sources where more detailed descriptions of security advice are available.

Design and organization

The design and layout of the security web pages vary. Some web pages are more daring in use of colors, pictures and different fonts, but each assessed web page is organized, professional-looking and pleasant to browse. All banks scored high in this category.

As the table shows, all provided links on the web pages are worthy and working properly, however, one link at OP Financial Group's web page was not working at the moment of the evaluation, and for this reason the bank scored lower in this category.

User-friendliness

In general, each website is effortless to move around and in most of the banks the security web page is easy to find within a reasonable time frame. Major navigational problems were not present. However, as the table shows, websites of Savings Bank and Ålandsbanken are slightly more difficult to use, and the advice is more difficult to find, as the user has to know what to look for from their website because the banks do not have a link to the security page on their front page. In order to find information about CNP-frauds the user has to browse several pages before being lead to the security page. Due to these reasons Ålandsbanken and Savings Bank scored lower than the other banks. In comparison, Danske bank's security advice is found in several locations on the website, which is convenient if the user is not primarily looking for security advice. By dividing the advice to several locations the bank is aiming to increase the possibility that customers will reach the information.

Total scores

The total scores were calculated by adding all the scores together and dividing by the numbers of indicators. Scores for each of the indicators are equally weighted, and the results are rounded to the nearest whole or half. As Figure 5. shows, Nordea, Danske Bank and OP Financial Group receive totals scores of three. S-Bank, Savings Bank and Ålandsbanken receive a total score of two.

Interview analysis

The interview resulted in five identified themes and these are detailed below.

Theme 1: The interest of preventing CNP-frauds

CNP-frauds have not reached Finland in the same extent as other Western countries, however, the problem is existing and growing rapidly. One possible reason for why CNP-frauds are not as common as in other countries is that Finnish customers are split between several smaller banks. The majority of banks in Finland are small (i.e. under 5 million customers), and banking customers have spread out between these small banks, making them more uninteresting to phishers who are trying to reach as many customers as possible. A great amount of phishing messages in English and Swedish reach the Finnish customers, but these are not as effective as phishing messages written in Finnish.

From Danske Bank's point of view, the monetary loss from CNP-frauds is not seen as a huge concern, and for this reason preventing these crimes is not a top priority for the bank at the moment. However, the increasing amount of sophisticated phishing emails written in Finnish is concerning the interviewee. Being a midsize bank, Danske Bank does have strategies for preventing CNP-frauds because its customers regularly fall victim for this type of crime. Many smaller banks, however, might not have a strategy for CNP-frauds, as their customers have never been targets. The lack of strategies would make smaller banks particularly vulnerable targets especially for phishing attacks.

Theme 2: Finnish banks generally try to pass on the liability to their customers

When a CNP-fraud occurs bank customer assumes that the lost money is charged back regardless whether or not customer has been negligent. Liability allocation is usually determined on a case-by-case basis. According to the current Finnish guidelines, the customer is liable for all losses in case of gross negligence, although in some cases it is difficult for a bank to prove that the customer has been negligent. However, it appears that the liability trend is changing. According to the interviewee, some Finnish banks cover all the losses no matter the level of negligence. The losses might even be covered on several occasions to the same customer in cases where the customer falls victim for CNP-fraud due to his own actions. This behavior increases the costs for the bank, but these costs are considered bearable.

According to the interviewee, in cases of man-in-the-middle attacks (for definition, see Appendix 1) banks generally are willing to cover the monetary losses. However, the liability allocation becomes a problem when customers lose money as a result of entering a phony online banking website via phishing e-mail. The phony website is perceived as a real one, and therefore the customer automatically assumes bank being responsible and absorbing the monetary losses. When signing payment card contract terms, customers agree not to give their payment card details or online banking details to third parties, and according to the interviewee many banks inform their customers about this responsibility on their web pages. From Danske Bank's point of view, by informing customers about their responsibilities to keep their confidential data safe the bank is aiming to push the liability towards customers. However, this trend slowly appears changing as a result of negative publicity banking industry is receiving in Finnish

media, and the third-party organizations dealing with consumer complaints changing the liability allocation to customer's favor.

The guidelines by The Federation of Finnish Financial Services state that banks should not contact their customers by e-mail, but bank marketing department at Danske Bank sees e-mails as a great channel for approaching and informing customers about upcoming events and news. This conflict of interest is seen as a threat by the security department at Danske Bank because customers should not become adjusted to being contacted by e-mail. This secures that the bank is able to push the liability towards their customers: in cases of phishing attempt customers should be aware that the bank does not contact them by e-mail. However, the guidelines are recommendations, and it is possible that banks are deviating from them, but Danske Bank experiences that The Federation of Finnish Financial Services is actively pushing them to follow their guidelines, which has made Danske Bank more afraid to adopt new preventive strategies, especially if they are not recommended by the guidelines.

Theme 3: Finnish bank customers do not have enough knowledge about CNP- frauds

Older people who are not familiar with computers and those who are naïve and irresponsible in security protection of their computers are at high risk for falling victim for CNP-fraud, particularly phishing. CNP-frauds are difficult to comprehend, and Finnish bank customers are missing crucial information about CNP-frauds. The interviewee finds the lack of knowledge as the main reason why customers do not understand when they are responsible for the abuse of their payment cards. CNP- frauds are seen as a result of weak bank security rather than a result of irresponsible online behavior.

Stakeholders dealing with payment frauds are not cooperating, and it lies on banks' responsibility to educate their customers. Danske Bank is convinced that they are doing enough to bring CNP-frauds down to acceptable levels, and the bank tries to educate its customers about their responsibilities online and when customers visit their office. To make the matters worse, Finnish bank customers are not taking the initiative to educate themselves, although information is available in everywhere: newspapers, television, and internet. Danske Bank also offers a variety of advice on its website, but the interviewee experiences that it is not is reaching customers. Payment fraud losses occur so seldom that most consumers do not appreciate the risk to which they are exposed.

Theme 4: Bank customers are not willing to pay higher user charges for higher security

According to the interviewee, banks generally have little incentive to pursue additional security measures (e.g. blocking deviant transactions and more visible educating) despite the possibility to do so. The reason for this is unwilling customers: higher security level would include slower service and higher user charges. Although Danske Bank has strong security measures for protection of its customers, failure in user awareness practices hinders the bank from adopting more aggressive preventive actions. Due to their lack of knowledge about liability, bank customers of Danske Bank believe that their monetary loss will be covered by the bank, and for this reason customers do not demand higher security measures. Further, increasing the user charges would result in losing customers, so instead of focusing on creating and implementing security measures Danske

Bank chooses not to talk about CNP-frauds in order to not make customers concerned.

Theme 5: Reputation is important for Finnish banks
Banks have a continuing reputation in the business world to protect. The Finnish media is writing about CNP-frauds a lot in comparison to other more common forms of fraud, and Danske Bank is concerned about this media coverage, as it may show banking industry in a bad light and make bank customers concerned. This would result in loss of customers. Good reputation is crucial for banks, as their goal is to grow, and due to this, it is important to response in bank customers' needs. According to the interviewee, there is a need to follow the emerging trends and innovations, but the communication between the bank and customers is not quite working. There are no sure ways of preventing payment frauds, and the survival strategy is to go along with the other banks and avoid media coverage.

ANALYSIS

The institutional pressures in CNP-prevention

As Finnish bank customers use Internet and online banking services exceedingly, it has increased the institutional pressure for banks to provide sufficient safety to their customers against the various cyber security threats. In order to survive in the uncertain environment of CNP-prevention many banks are taking actions in customer awareness education to address this type of crime. By providing this information and advice banks constitute their own form of regulation to which they hope customers will react positively.

The web page assessment of banks' security advice indicates that the majority of the banks offer their customers information about safe payment card use and safe online behavior as well as the most common means of CNP-fraud, or alternatively refer to external sources where the same information can be obtained. Like other Finnish banks, Danske Bank is aware of the emerging threat of CNP-frauds and offers advice to its customers. According to Danske Bank, phishing in particular is an increasing concern, and the attacks are becoming more and more sophisticated, affecting especially older customers who might not have as much knowledge about how to stay safe online as younger customers, and who might struggle with comprehending payment frauds. This concurs with the results from the webpage assessment: the majority of the banks are responding to this problem by providing information about phishing that can be obtained from user-friendly web pages that are easy to understand and navigate. Based on the interview, malware and data breaches do not seem to be as great concern for Danske Bank as phishing, however, the webpage assessment indicates that it is popular among banks to provide advice about malware - nearly as common as providing advice about phishing.

It seems that the uncertain environment of payment fraud prevention leads banks to mimicking each other's practices – or the lack of practices. This dependency on each other is a sign of institutional isomorphism, either normative or mimetic: this norm of advising customers has either been considered convenient by the whole market, or has been first adopted by the dominant institutions in the market.

However, some of the banks disobey the isomorphic pressure to advice their customers, which demonstrates immunity for the institutional norm. As the web page quality assessment shows, two of the banks did not provide any information regarding CNP-fraud on their web pages. Further, the use of several formats, such as video, as supporting technique for presentation indicates that some banks ignored the institutional norm to provide information only in text format. Also, banks differed in the use of different languages: besides Finnish, a few banks offered information in English and Swedish. As reported by Danske Bank, a great amount of phishing messages written in English and Swedish reach Finland, and for this reason it is highly important to provide advice in these languages in order to educate those who might fall for these phishing messages. Again, this demonstrates how banks are split between institutional norms.

In comparison, Finnish banks seem to be considerably homogenous in presenting information about the rules of liability. The majority of the banks do not provide enough information about their rules regarding the liability allocation: the obligation to keep payment card details safe is the only advice that can be obtained from the banks' security webpages. It seems that there exists a form of institutional pressure to not to educate customers to an extent where they are be able to understand their responsibilities in cases of CNP-fraud. Again, this practice is considered to be convenient by the majority of the institutions in the environment, or has become a standard as a result of the dominant institutions adopting it. Adopting this practice has lead to a liability distribution conflict between the banks and their customers. According to the interview with Danske Bank, the uneducated customers hold banks responsible when they suffer monetary losses due to CNP-fraud, while bank is acting in self-interest and tries to push the liability towards customers. This finding concurs with the results of Koivunen & Tuorila (2015) who recognised the same issue after studying Finnish complaint documents sent to a third-party organization.

Educating customers via Internet – a complete but non-effective security solution on the problem of CNP-fraud

Based on the web page assessment, it can be concluded that the advice available online is easy enough to find and comprehend, and enough to give an accurate picture of the most common means of CNP-fraud. This information is sufficient enough to educate Finnish bank customers to an extent where they should be able to know how to protect themselves from CNP-frauds. Despite the amount of information, there seems to be lack of customer awareness in respect of this type of crime. According to Koivunen & Tuorila (2015), the use of online banking has increased steadily, while the proportion of Finnish Internet users who are aware of cyber threats remain unchanged. This proposes that most of the customers engage in online banking without sufficient awareness on potential dangers of Internet. Customers who believe they have little knowledge of the cyber environment, online banking services and security often feel that it is too difficult to contribute to their own online safety (Milne et al., 2009). Likewise Koivunen and Tuorila, Danske Bank is concerned about the uninformed customers as it experiences that the advice distribution between the bank and its customers is poor. Despite the amount of information that is available online, it seems that the risk of falling victim for CNP-fraud is not enough as incentive for the bank customers to take the initiative to educate themselves about payment frauds.

DISCUSSION

The crux of the problem: self-interested infrastructure of banking industry

The explanation for Finnish banks' performance in providing advice against CNP-frauds lays in their infrastructure. The rapid growth of banking system has changed the nature of retail banking radically by increasing the competition on the market (Nätti & Lähteenmäki, 2016), and as a strategy to survive, banks are increasingly aiming to gain legitimacy. Competing for legitimacy is leading banks to a strong aspiration to gain and maintain their value on the market, which results in signs of regulatory capture and confusion in how to respond to the increasing problem of CNP-fraud.

Feeling pressure to deal with the increasing and changing competition on the market, banks' investments in providing advice to their customers are a result of the institutional pressures, and therefore can be seen as a way of protecting public image and ensuring market value rather than a personal interest in engaging in CNP-prevention for the sake of public good. This self-interested infrastructure is a sign of banks being unable to manage the amount of uneducated customers. In point of fact, the differing institutional norms in educating customers and the lack of common guidelines in CNP-prevention are increasing the competition between Finnish banks by making the retail banking market more unsecure.

The unwillingness to provide information about liability allocation also indicates Finnish banks being under the impact of regulatory capture. Banks are aware of customers lacking incentives to educate themselves about liability rules but do not show interest in properly undertaking the problem. This is because of providing advice, regardless if it is complete, comprehensive and up-to-date, is assuring banks legitimacy. This aspiration for legitimacy results in failure in user awareness practices and banks' attempts to push liability towards their customers. Interestingly, some banks do cover the monetary losses in cases of CNP-fraud no matter the level of customer's negligence. This, however, can be interpreted as another type of self-interested behavior. Banks' negative responses to compensating customers' monetary losses turn the uneducated customers' trust towards banks into distrust (Douglas, 2009; Koivunen & Tuorila, 2015), and as an quick and easy panacea to maintain their legitimacy, banks are choosing to cover their customers' losses. Assuring customers zero liability is supported by arguing that it is encouraging banks to invest more time, money and effort in to fighting against payment frauds (Levitin, 2010). However, responding to the demand of the public does not encourage banks to devote to providing information about liability nor support customers' motivation in learning about CNP-frauds and their responsibilities as banking customers. Assuring zero liability does not solve the root problem of uneducated customers, as they become accustomed to banks absorbing their losses. Therefore it might bear a risk for both parts becoming more passive if customers are not liable for their – even grossly negligent – actions. As Cooter & Rubin (1987) state, liability allocation that does not influence ideal behaviour for both parties is worthless - the aim of liability allocation is to give both parties enough incentives to act optimally.

One reason why banks are not engaging in more effective CNP-fraud prevention is because the payment system was designed for them. This is allowing banks to continue controlling to pursue their own institutional interests, as banks will always be controlling the infrastructure of industry (Segal et al., 2011:749). In fact, CNP-frauds might be something banking industry does not want to prevent. Banks are profiting from card transactions, regardless of whether they are fraudulent, and when covering unauthorized payments, banks shift much of the costs back to the merchant who sold the fraudulent goods (Segal et al., 2011:749, 773). This suggests that CNP-frauds are offering banks an opportunity for financial growth with the cost of public good, which makes it challenging for banks to engage in truly effective CNP-fraud prevention.

This type of institutional environment allows banks to create a self-interested regulation and to continue behave in self-interest. Outcomes of such a strong regulatory capture will bear a risk for counterproductive results, and this indicates that banks alone are not able to carry the responsibility of protecting customers from the risks of CNP-fraud.

Discussion of methodological limitations

Literature review

Firstly, the literature review was not intended to be fully comprehensive in regard to the means of CNP-fraud as the review was limited to defined scope of research. Inclusion and exclusion criteria were designed secure that relevant and high quality literature is included, and it is possible that these criteria excluded important literature within the research area. The literature sample was limited to quite wide time frame, wherein lies a risk for choosing out-dated literature. This issue was tried to overcome by using multiple sources published in different years.

Web page quality assessment

Firstly, the web page quality assessment focused mainly on the quality of the content rather than visual design characteristics. However, it is unclear to which extent the appearance of a banks' web page impacts its users. In fact, web page might be a key factor in influencing users perceptions and behaviors (Flavian et al., 2009). Based on the visual characteristics, bank customers form an opinion about the security web page that determines their opinion about the page, and based on this opinion they choose to stay or leave. Thus, the design elements of a bank's web page might require more attention than this research expected. In fact, banks' security content might be becoming increasingly visual – videos and illustrations a few of the banks used to enhance their presentation were an example of how banks can use visual attraction to connect with their customers.

Secondly, this study focused on the advice that is available through banks' web pages and excluded the advice that customers receive via online banking services or by physically visiting a bank office. It is possible that Finnish banks provide more or different type of advice through these channels than through their web pages, and this makes it more difficult to determine to what extent banks are engaging in educating their customers about CNP-frauds.

Lastly, one major limitation is that the web page quality assessment did not involve user testing nor use of multiple evaluators. Instead, it was based on one evaluator's interpretation of how users interact with the web page, i.e. each evaluated aspect was a matter of subjectivity. In order to find actual problems users might face while trying to find the advice and while they are reading the advice the web page must be tested with representative people, or alternatively by using several evaluators.

Qualitative interview

Despite using the guidelines by Miller-Adams and Myers (2003) and studying the technical language of banks, it is possible that the interviewee was not comfortable enough to provide as complete answers he would have provided to a interviewer who is more familiar with the Finnish banking industry.

Additionally, interviews in banking industry may be dependent on where within the bank the interviewee is working (Miller-Adams & Myers, 2003). The interviewee in this study is not an expert in all areas, and it is reasonable to assume he may be influenced by some degree of self-selection. However, by using semi-structured interview, it was secured that the interviewee was able to focus on those areas he has most expertise on.

Despite the limitations, approaching the research topic by using qualitative operates as an important complement to the literature review and the web page quality assessment. It would have been difficult to obtain information within the field through other methods.

CONCLUSIONS

This study took a multilayered approach to CNP-frauds in Finnish context by using two theoretical perspectives, neo-institutional theory and regulatory theory, in order to look at the banking industry's incentives to confront this type of crime. By examining the literature about CNP-frauds, assessing the quality of banks' online advice and interviewing a security expert within the Finnish banking industry a more detailed insight of the issue of CNP-fraud prevention was accomplished. This study has demonstrated the importance of understanding the factors that impact the prevention of CNP-frauds in banking environment, leading to a better understanding of the institutional pressures within the banking industry.

The results of this study indicate that the banks' desire for legitimacy might not be compatible with caring for public good. Lacking information about CNP-frauds, Finnish banking customers are at high risk for falling victim for this type of crime, and balancing between common good and self-interest and being under the strong system of institutional norms the banking industry do not seem to know whether to respond and how to respond to this problem.

Being a significant issue for both criminological and economical field, effective CNP-fraud prevention requires active involvement from all of the actors in the chain. Cooperation among banks, police and third-party organizations embraces new ways of working and innovations, and most importantly it might allow type of institutional change that is creating the right incentives for banks to engage in

payment fraud prevention. Collaboration between banks is specifically important, as it helps banks to put aside the competition, and the strong relationships between competitors might become a low-cost direction in preventing CNP-frauds. The banking industry needs to take action and introduce new solutions for educating customers and identify the best practices to mitigate this type of crime from customers' point of view. By ultimately combining their strengths banks might have a chance to win the game against payment frauds.

Further, strengthening the institution-public relationship might be a key factor in effective CNP-fraud prevention. Customers should be included as active participants in CNP-prevention in order to create a regulation that they are likely to respond positively to. Through this interaction mutual trust is built, and that trust could translate into both engagement in fighting against this type of crime and enhancement in banks' legitimacy. Most importantly, both national and international measures should be considered in order to tackle the threats in the rapidly evolving cyber environment.

Future research

Future research can expand upon these characteristics of banking industry and elaborate further the relationships between the institutional environment of Finnish banks and effective CNP-fraud prevention. The limitations of this study are an opportunity to make suggestions for further research. More comprehensive interview data from several banks' point of view needs to be collected in order to achieve a deeper understanding of the foundation of regulatory capture within Finnish banking industry. Additionally, a web page assessment based on the perceptions of a multidisciplinary group of experts could identify the key factors that influence the degree of success of security web pages. In the interest of achieving a more detailed insight on how banking customers' behavior is influenced by the banking web page, it is necessary to include viewpoints of banking customers. These suggestions might help us to go forward in answering the question 'who pays?'

REFERENCES

Ablon, L., Libicki, M. C. & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hacker's bazaar*. National Security Research Division, 2014.

Bakir, C. (2013). *Bank Behaviour and Resilience: The Effect of Structures, Institutions and Agents*. London: Palgrave Macmillan.

Blencowe, A. (2012). Korvausvastuu kiinni asiakkaan huolellisuudesta. *YLE Uutiset.* [online].
Available at: http://yle.fi/uutiset/3-5053033 [Accessed 20 February 2017].

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2). pp. 77-101.

Bryman, B. & Bell, E. (2007). *Business Research Methods*, 2nd ed., Oxford: Oxford University Press.

Cassim, F. (2015). Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thiefs? *Potchefstroom Electronic Law Journal*, 18(2).

Cooter, R. D. & Rubin, E. L. (1987). A Theory of Loss Allocation for Consumer Payments. *Texas Law Review*, 63 (1987).

Creti, A. & Verdier, M. (2014). Fraud, Investments and Liability Regimes in Payment Platforms. *International Journal of Industrial Organization*. vol. 35, pp. 84-93.

DeJordy, & Jones, (2008). *Institutional legitimacy* in Clegg, S. & Bailey, J. R. (2008). International Encyclopedia of Organizational Studies. SAGE Publishing.

Denscombe, M. (2010). *The Good Research Guide: For Small-Scale Social Research Projects*. McGraw-Hill.

Dhameja, S., Jacob, K. R. & Porter, R. D. (2013). Clarifying Liability for Twenty-First-Century Payment Fraud. *Economic Perspectives*, 37(3), pp.107-129.

DiMaggio, P. J. & Powell, W. (1983). "The iron cage revisited" institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48 (1983), 147-60.

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

Directed 2008/48/EC of the European of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC.

Engebretson P. (2011). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier; 2011.

Enoch, Y. S., John, A. K & Olumuyiwa, A. E. (2013). Migitating Cyber Identity Fraud Using Advanced Multi Anti-Phishing Technique. *International Journal of Advanced Computer Science and Applications,* 4(3), pp. 156-164.

Esposito, R. & Ryan, J. (2010). Police: Eastern European Crime Ring Stole Millions Using Computer Virus. *ABC News*. [online]
Available at: http://abcnews.go.com/Blotter/zeus-trojan-virus-eastern-european-crime-ring-allegedly/story?id=11766688 [Accessed 15 April 2017].

European Consumer Centres Network (ECC-Net) (2014). *Chargeback in the EU/EEA: A solution to get your money back when a trader does not respect your consumer rights.* [online]
Available at: http://ec.europa.eu/consumers/ecc/docs/chargeback_report_en.pdf [Accessed 3 March 2017].

Europol (2016a). *Internet Organized Crime Threat Assessment (IOCTA) Annual assessment report.* [online]
Available at: https://www.europol.europa.eu/iocta/2016/ [Accessed 16 January 2017].

Europol (2016b). *Darknets and hidden services*. [online]
Available at: https://www.europol.europa.eu/iocta/2016/darknets.html [Accessed 20 January 2017].

FINE (2016). *Näitä asioita käsittelemme*. [online].
Available at: https://www.fine.fi/tietoa-finesta/riita-asiat/naita-asioita-kasittelemme.html [Accessed 2 March 2017].

Flavian, C., Gurrea, R. & Orus, C. (2009). Web design: a key factor for the website success. *Journal of Systems and Information Technology*, 11(2), pp.168-184

Gehanno, J. F., Rollin, L., Darmoni, S. (2013). Is the coverage of Google Scholar enough to be used alone for systematic reviews?. *BMC Medical Informatics and Decision Making*, 13(7).

Grazioli, S. & Jarvenpaa, S. L. (2000). Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans.* 30 (4), pp. 395 – 410.

Heikkinen, P. & Iivarinen, T. (2011). Ensuring trust in electronic payment media. *Journal of Payments Strategy & Systems*. 5(2), pp. 161-168.

Haddaway, N. R., Collins, A. M., Coughlin, D. & Kirk, S. (2015). *The Role of Google Scholar in Evidence Reviews and its Applicability to Grey Literature Searching*. PLoS ONE 10(9): e0138237.

Hardy, D. C. (2006). *Regulatory Capture in Banking. International Monetary Working Paper.* International Monetary Fund, WP/06/34, 2006.

Hasan, L. & Abuelrub, E. (2011). Assessing the quality of web sites. *Applied Computing and Informatics*. 9 (1), pp.11-29.

Institute of Criminology and Legal Policy (KRIMO) (2015). *Rikollisuustilanne: Rikoskehitys tilastojen ja tutkimusten valossa*. Katsauksia 16/2016.

Internet World Stats (2016). *Internet in Europe stats*. [online]
Available at: http://www.internetworldstats.com/stats4.htm [Accessed 1 March 2017].

Interpol, (n.d.). *Financial crime*. [online]
Available at: https://www.interpol.int/Crime-areas/Financial-crime/Financial-crime [Accessed 15 March 2017].

Investopedia, (n.d.). *Commercial bank* [online].
Available at:
http://www.investopedia.com/terms/c/commercialbank.asp#ixzz4g8Tl7Q6J [Accessed 20 April 2017].

Investopedia, (n.d.). *Electronic commerce – e-commerce* [online].
Available at:
http://www.investopedia.com/terms/e/ecommerce.asp [Accessed 20 April 2017].

Junger, M., Montoya, L. & Overink, F. J. (2016). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior* 66 (2017), pp. 75-87.

Kessem, L. S. (2012). Phishing in Season: A Look at Online Fraud in 2012. RSA, 2012. [online]
Available at: https://blogs.rsa.com/phishing-in-season-a-look-at-online-fraud-in-2012/ [Accessed 29 January 2017].

Koivunen, T. & Tuorila, H. (2015), Consumer trust relations with payment cards and banks: an exploratory study. *International Journal of Consumer Studies*. vol. 39, pp. 85–93.

Levine, M. E. & Forrence, J. L. (1990). Regulatory Capture, Public Interest, and the Public Agenda: Toward a Synthesis. *Journal of Law, Economics, & Organization*, vol. 6, pp. 167-198.

Mahdi, M. D. H. & Rezaul, K. M. (2012). *Detecting fraud in E-business system: An information security perspective on the banking sector in UK* in Gupta, M. (2012) "Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions".

Meyer, J. W. & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*. 83, pp. 340–363.

Monahan, T. & Fisher, J.A. (2015). Strategies for Obtaining Access to Secretive or Guarded Organizations. *Journal of Contemporary Ethnography*, 44(6), pp. 709–736.

Moustakis, V. S., Litos, C., Dalivigas, A. & Tsironis, L. (2004). *Website quality assessment criteria*. Ninth International Conference on Information Quality (IQ 2004), November 5-7, 2004.

Miller-Adams, M. & Myers, C. T. (2003). *Breaking into the Bank: The Challenge of Gaining Meaningful Access to the World Bank* in Feldman, M. S., Bell, J., & Berger, M. T. Gaining access: a practical and theoretical guide for qualitative researchers. Rowman Altamira, 2004.
Milne, G. R., Labrecque, L. I., and Cromer, C. 2009. Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, 43(3), pp. 449-473.

Mäntymaa, E. (2015). Suomen suurin tietovuoto yhä selvittämättä – esittelyssä kuusi suurta kyberrikosta. *YLE Uutiset*. [online]
Available at: http://yle.fi/uutiset/3-7795604 [Accessed 13 April 2017].

Namey, E., Guest, G., Thairu, L. & Johnson, L. (2008). *Data Reduction Techniques for Large Qualitative Data Sets*. In Guest, G. & MacQueen, K. Handbook for Team-based Qualitative Research. Rowman Altamira.

Nätti, S. & Lähteenmäki, I. (2016). The evolution of market orientation in Finnish retail banking – from regulation to value creation. *Management and Organizational History*. 11(1), pp. 28-47.

OECD (2011). *Regulatory Policy and Governance: Supporting Economic Growth and Serving the Public Interest*. OECD Publishing. [online]
Available at: http://www.oecd-ilibrary.org/governance/regulatory-policy-and-governance_9789264116573-en [Accessed 8 March 2017].

Official Statistics of Finland (OSF) (2016a). *Statistics on offences and coercive measures. 3rd Quarter 2016*. Helsinki: Statistics Finland. [online] Available at: http://www.stat.fi/til/rpk/2016/03/rpk_2016_03_2016-10-18_tie_001_en.html [Accessed 16 March 2017].

Official Statistics of Finland (OSF) (2016b). *Use of information and communications technology by individuals.* Helsinki: Statistics Finland [online] Available at: http://www.stat.fi/til/sutivi/2016/sutivi_2016_2016-12 09_tie_001_en.html [Accessed 13 April 2017].

Segal, L., Ngugi, B. & Mana, J. (2011). Credit card fraud: a new perspective on tackling an intransigent problem. *Journal of Corporate & Financial Law*, 16, pp.743–781.

Shekokar, N. M., Chah, C., Mahajan, M. & Rachh, S. (2015). An Ideal Approach for Detection and Prevention of Phishing Attacks. *Procedia Computer Science*. vol. 69, 2015. pp. 82-91.

Statista (2016). *Online banking penetration in selected European markets in 2016.* [online] Available at: https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/ [Accessed 1 March 2017].

Stigler, J. G. (1971). The Theory of Economic Regulation. *Bell Journal of Management Science*, 2 (1), pp. 3-21.

Sutcliffe A. (2002). *Assessing the reliability of heuristic evaluation for web site attractiveness and usability*. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Jan. 2002.

Symantec (2008). *Underground economy report* [online]. Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf [Accessed 20 January 2017].

Symantec (2016). *Internet Security Threat Report (ISTR).* Volume 21, April 2016.

Thornton, P. H. (2011). *Isomorphism* in Teece, D. J. & Augier M. (ed.) The Palgrave Encyclopedia of Strategic Management. Palgrave Macmillan Publishers, 2011.

Wesley, K. W. (2004). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management. *Journal of Economic Crime Management*. 2(2).

Wren-Lewis, L. (2010). *Regulatory Capture: Risks and Solutions*, in Estache, A. Emerging Issues in Competition, Collusion, and Regulation of Network Industries. London Publishing Partnership, 2011.

YLE Uutiset (2012). *Vakava tietomurto – tuhansien suomalaisten tiedot vuotivat internetiin*. [online].
Available at: http://yle.fi/uutiset/3-5448332 [Accessed 20 April 2017]

APPENDIX 1. WORD LIST

ADR. A public third-party organization dealing with consumer complaints. Consumer Disputes Board (CDB) and the Banking Complaints Board (BCB) are the two Finnish equivalents of ADR (European Consumer Centres Network, 2014; Koivunen & Tuorila, 2015).

Authorization. During the process of authorization, a merchant obtains permission from the bank that issued the card to accept the card for payment.

Chargebacks. Full reversal of transactions by card issuers (Douglas, 2009).

Darknet. Anonymous networks often used as communication and marketing forum for cybercrime (Europol, 2016b).

Data breaches. Data breaches, also known as data leaks, refer to unauthorized access to a system of confidential information by an individual or group. Data breaches are one of the most common reasons for payment card abuse (Europol, 2016a; Symantec, 2016).

Electronic commerce (e-commerce). A type of business model for conducting business over electronical platforms, usually Internet (Investopedia, n.d.)

Hacking. Hacking is accessing information assets without proper authorization by thwarting security mechanisms (Dhameja et al., 2013).

Identity fraud. A type of crime where another person's personal data is used for harmful purposes, typically for economic gain (Cassim, 2015).

Identity theft. A type of crime in which a person's personal data is wrongfully obtained. Identity fraud, however, is often but not necessarily the consequence of an identity theft, and it refers to the use of another individual's confidential information for harmful purposes (Cassim, 2015).

Malware. A harmful software that is able to enter a system without authorisation. Includes viruses, worms and Trojans (Symantec, 2016).

Man-in-the-middle. An attack in which a cybercriminal is able to read, insert, and modify messages between two users or systems (Symantec, 2016).

Phishing. A deceptive attempt to scam people into disclosing confidential information by using false emails or text messages that appear to come from legitimate enterprises. These messages may contain harmful software or spyware or links to infected web pages (Enoch et al., 2013; Symantec, 2008).

Social engineering. A non-technical method for gathering personal information about a target through a process of exploiting flaws in human logic, i.e. cognitive biases (Engebretson, 2011).

Spoofing. An attempt to gain unauthorized access to a user's system or information by pretending to be the user. The main purpose is to trick the user into

releasing sensitive information in order to gain access to one's bank account or to steal personal information (Investopedia, n.d.)

Spyware. A software usually distributed by e-mail that is used to commit identity theft. By capturing information typed into computer keystrokes, spyware gains access to user's confidential information without the user's knowledge (Symantec, 2016).

APPENDIX 2. PHISHING E-MAIL EXAMPLE

From:
no_reply@emailonline.yourbank.com
Subject: Account Status

Dear (Your Bank) Customer,

Due to recent activity on your account, we have issued the following security requirements. For your security, we have temporarily prevented access to your account. (Your Bank) safeguards your account when there is a possibility that someone other than you tried to sign on.

You may be getting this message because you signed in from a different location or device. If this is the case, your access may be restored when you return to your normal sign on method. For immediate access, you are required to follow the instruction below to confirm your account in order to secure your personal account informations.

Click To Confirm Your
Account Regards, Carter
Franke

Chief Marketing
Officer Card
Member Services

source: https://us.norton.com/bank-email-scams/article