TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Markus Suvanto

SHIFTING OF BURDEN OF PROOF BY CIVIL COURTS IN ASSESSMENT OF ELECTRONIC EVIDENCE

Bachelor's thesis

Programme HAJB08/14 – Law, specialization on European Union and International Law

Supervisor: Agnes Kasper, PhD

Tallinn 2018

I declare that I have compiled the paper independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not been previously been presented for grading.

The document length is ……... words from the introduction to the end of summary.

Markus Suvanto ……

Student code: 156139 HAJB

Student e-mail address: suvantojr@gmail.com

Supervisor: Agnes Kasper, PhD …….

The paper conforms to requirements in force

Chairman of the Defence Committee:

Permitted to the Defence

……..

TABLE OF CONTENTS

ABSTRACT

The aim of the research is to analyze both the approach taken by courts leading to incorrect shifting of burden of proof and negligence of parties in relation to insufficient customs of courts to process the electronic evidence. The hypothesis of this research is that courts are shifting the burden of proof from the bearer of electronic evidence leading to an arguable decision favoring of another party. Occasionally a dispute arises between service provider and an individual when court analyses electronic evidence and the facts of the situation. Usually when the unauthorized access or frauds have happened, the legitimate owner has suffered financial or other unpleasant losses. In such situations, courts should approach the matter with certain standards and methods without giving value to other party's position on the expense of the facts of the case, while at the same time giving an interpretation of law in a way that no mistreatment is applied and that the court proceedings have been addressed equally towards both parties.

Keywords: electronic evidence – civil law – burden of proof – unauthorized use – credit card - liability

ABBREVIATIONS

CJP	Code of Judicial Procedure 1.1.1734/4.
BGH	Federal Supreme Court of Justice (Germany)
EU	European Union
EIA	Electronic Identification Act - Law on Strong Electronic Identification and Electronic Signatures.
FINE	Finnish Financial Ombudsman Bureau
KKO	Supreme Court of Finland
KouHO	Court of Appeal of Eastern Finland
PLA	Payment Liability Act.
PSA	Payment Services Act.

INTRODUCTION

I chose this topic because of the fascinating possibility of courts to shift burden of proof based on incorrect interpretation of law caused by lack of knowledge towards electronic evidence.

Following research questions are used on the research of this thesis:

Are civil courts shifting the burden of proof away from the proponent of electronic evidence?

What are the relevant standards for determining reliability of electronic evidence?

Is there a problematic approach applied by civil courts on situation of unauthorized use of credit card?

The aim of the research is to analyze both the approach taken by courts leading to incorrect shifting of burden of proof and negligence of parties in relation to insufficient customs of courts to process the electronic evidence. Status and importance of electronic evidence is approached by expressing controversies of parties on situation of unauthorized access of credit card or online payments services.

A distinction is made between foreign and Finnish legal customs by analyzing relevant arguable case law. Qualitative methods and traditional legal analysis supported with law in force will be used on process of the research. Explanatory method provides different levels of comparison within case-law, legal doctrines and principles to strengthen the topic with relevant material.

The structure of the thesis is following:

The first chapter will contain special characteristics and explain the deviance of electronic evidence in comparison to analogical evidence. Fundamental requirements and complexity of admissibility of electronic evidence are presented shortly, but with a clear manner.

The second chapter will express multinational case law with distinct court approaches. Author pursues to clarify the twisted approach of courts and reasons that some courts have not been able to treat proceeding parties with equal customs. Imprudent reliance on presented evidence without questioning and scope of negligence are included with the analysis.

The final chapter explicates alternative options and further analysis-based thoughts for altering the course taken by some courts and to improve the knowledge and elements of electronic evidence itself, to accomplish a more certain, obvious and advanced interpretation of law. Author seeks to establish justified solutions against likelihood of court's failure to ascertain the authenticity of electronic evidence.

Different case law and decisions from Finnish Supreme Court (KKO) and other courts are demonstrated along with ruling recommendations from financial or administrative parties. The Payment Liability Act (PLA), Payment Services Act (PSA) and Law on Strong Electronic Authentication and Electronic Signatures (EIA) along with Code of Judicial Procedure(CJP) together form the relevant regulations for the topic.

The sources for this thesis are gathered from legal text books and legal articles, that provide essential views and observations, latest or most argued issues as well as controversial statements and visions.

1.CHARACTERISTICS OF ELECTRONIC EVIDENCE

The digitalization of modern world produces electronic data and elements that may be used as evidence on civil or criminal court proceedings. Electronic evidence represents its own characteristics, ways of use and differs a lot from traditional evidence, but still is regulated under same rules and laws provided by legislation.

The evidence has an extremely important feature in court proceedings on modern legal jurisdiction. In addition to its key elements, such as method of proof, best rule evidence, hearsay, expert witnesses and free assessment of evidence and free disposition, it is important to be able to observe the difference between analogical and digital evidence and to handle these forms of evidence with correct methods.[1] The main differences between digital and analogical evidence is the difficulty to estimate whether or not the evidence is admissible, because for analogical evidence, such as paper document or comparable item, the process for admissibility and authenticity is more distinct.[2] This is because the modern technology enables the possibility of computing and modification of evidence in a way, that makes it really hard to prove the origin of evidence and that no single detail was modified to different form. If lost or contaminated data is not identified or there are doubts of contamination, the burden of proof for the origin and reliability of evidence is with the party expressing the evidence. The opposite party may question the origin, reliability and the methods the evidence was gathered with, such as lawfulness and authenticity as well as the purity of the whole sequence of the gathering of evidence.[3]

The transformation of details of certain data or piece of evidence may happen without purpose, it is easy to occur and does happen relatively often in today's world, but still for evidence to be admitted and fulfill the evidentiary obligations, it is important that the origin of evidence can be proven in a solid and comprehensive way.

---

[1] Koulu, R. (2015). *Evidence in Civil Law - Finland*. Slovenia: Institute for Local Self-Government and Public Procurement. p 2.

[2] Mason, S., Seng, D. (2017). *Electronic Evidence*. 4th ed. London: University of London. p 48

[3] Bell, Graeme B. and Boddington, Richard (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? *Journal of Digital Forensics, Security and Law*: Vol. 5, No. 3, Article 1. p 3

A clear definition of electronic evidence without gaps is a really hard task and far from simple. In general, electronic or digital evidence is any data which is stored on some type of device, such as computer, phone, tablet, software or platform which does produce or handle information or other content in a way that it can be presented as evidence in court or during an investigative process.[4] There are many other variations of the definition of electronic evidence, such as the one given by Eoghan Casey, the author of books relating to computer crimes and digital evidence. He defines electronic evidence as: "*any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi."*[5] Stephen Mason and Daniel Seng, famous authors on area on electronic evidence, have proposed following unambiguous definition:*"data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence."*[6]

Even that definitions of electronic evidence differ a lot from each other, they all contain similar elements. First element that has a strong prestige in definition of electronic evidence is 'data'[7], because it includes all aspects and forms of information and content and all possible ways the information can be applied through devices and programs which handle data. Second element is the use and transmission of the data which does cover the separate form of analogical evidence and outputs that are produced[8] and the third one is the restrictions and admissibility of the evidence which highlight the importance and impact of the evidence for the outcome of the court decision.[9]

---

[4] Mason (2017), *supra nota* 2, p 18

[5] Casey, E. (2011). *Digital Evidence and Computer Crime.* 3rd ed. USA: Elsevier. p 7

[6] *Ibid.*, p. 19

[7] *Ibid.*, p. 19

[8] *Ibid.*, p. 20

[9] *Ibid.*, p. 20

1.1. Admissibility of evidence

The general legal requirements to establish sufficient standards for admissibility of analogical evidence are regulated by laws, but they are not suitable or sufficient to legally cover data and devices that generate electronic evidence, because the differences and features of electronic evidence creates conflicts and evidentiary issues if governed by such laws.[10]Therefore, courts have applied different practices and means of interpretation of law towards evidence gathered or produced from digital sources.[11]

Huge judicial issue is the ease of manipulating of electronic evidence as the court has specific requirements and standards for evidence to be approved for court proceedings.[12] When evidence is obtained, it must be proven that that has happened with lawful manners and that the origin of evidence has not been altered or modified since it was gathered in the first place.[13] For the evidence to be incorporated for court proceedings, it must be reliable and complete, meaning that it is able to prove or disprove some claimed fact on the court and relates to addressed matter as well as not to lack any detail or feature, that could place other party in unfavorable situation or give a partial understanding to the matter.[14] On case *Lorraine v. Markel American Insurance Company,* the court was unsuccessful to identify the standards of admissibility of evidence and decision was not based on poorly presented evidence but on lack of understanding for the matter by court.[15]

For evidence to be admitted to court proceeding, it must be authentic, which means that it has to be able to be connected to the current matter in hand and often is required to prove that it was

[10] Thomson, L. L. (2013). Mobile Devices: New challenges for admissibility of electronic evidence. – *The SciTech Lawyer,* Volume 9, Number 3, p 1.

[11] *Ibid*., p. 2.

[12] Biasiotti, M.A. (2017). A proposed electronic evidence exchange across the European Union. – *Digital Evidence and Electronic Signature Law Review,* Volume 14, p 1.

[13] Goode, S. (2009). The Admissibility of Electronic Evidence. – *The Review Litigation,* Volume 29, Number 1, p 8.

[14] Casey (2011), *supra nota* 5, p 60.

[15] Thomson (2013), *supra nota* 10, p 3.

collected for that purpose only.[16] The court may also decide the evidence to be partially or totally excluded, if there are suspicions against the above-mentioned requirements. The best evidence rule has strong position in some legislations and means that the evidence must be presented on its original, unaltered form in same content and concept it was collected in the first place.[17] The rule can be approached from two viewpoints, first containing an idea that the best evidence will be used or secondly that all the evidences that are not the best ones will not be admitted to use of court on trial.[18]

Electronic evidence needs special methods and professional knowledge from evaluating persons and mistakes or improper handling should not happen, because otherwise the evidence may lose its value and to be concluded as inadmissible.[19] Investigators, lawyers and professional personnel must approach the evidence as being aware of that there could be errors or modification on the evidence, meaning that there is an overall chance for failure especially on the systems providing the electronic evidence.[20]

As decisions for admitting the evidence are left to the individual courts and under their interpretation, more serious problems stand in the way of more straightforward and liable admission of electronic evidence.[21] There are no strong, common international legislation regulating electronic evidence and slight legislation of certain countries make a huge difference for traditions of admissibility and interpretation of electronic evidence.[22] EU legal framework and guidelines may be applied in the absence of unified legislation, but they may create barriers, because of data privacy and cross border issues, and because of that additional special legislation

[16] Mason (2017), *supra nota* 2, p 193.

[17] Miller, C. (2012). *Evidence: Best Evidence Rule.*1st ed. USA: CALI eLangdell Press. p 3.

[18]Mason (2017), *supra nota* 2, p 49.

[19] Biasiotti (2017), *supra nota* 12, p 6.

[20] Mason (2017), *supra nota* 2, p 186.

[21]Kaplow, L. (2012). Burden of Proof. – *Yale Law Journal,* Volume 121, No 4, p 746.

[22]Biasiotti (2017), *supra nota* 12, p 3.

will be needed.[23] The legislation should also be up to date for it not to prevent development or use of technology.[24]

When we approach disputes between bank and an individual from bank's perspective and take into consideration the fact that the truth is hard to notice afterwards, but instead the procedural truth based on given statements and evidence will usually be the outcome we can agree that the bank has more leverage on such situation.[25] The banks have huge financial and professional resources in its use and in addition the bank have a legal right to use confidential information of the client and other measures as a creditor to obtain and secure the best outcome for the bank.[26]

1.2. Relevant case-law

Banks favor a procedure, where they lack providing informative details or restrict the number of evidence presented for court to shift the burden of proof towards the plaintiff. [27] As an objection for claim of damages the bank may counterclaim the plaintiff by accusing him for being neglect for security measures and this way indirectly leave the plaintiff in position where he has very little or impossible chances to prove his claims to be true.[28] On some situation the banks may claim that they have used every measure available to ensure the plaintiff's knowledge of instructions and rules of security of credit cards and their operative systems and accuse him for neglect behavior towards those.[29]

---

[23] *Ibid*., p. 6.

[24] *Ibid*., p. 6.

[25] Koulu (2015), *supra nota* 1, p 11

[26] Wuolijoki, S. Hemmo, M. (2013). *Pankkioikeus.* Finland: Talentum Oyj. p 53.

[27] Mason, S. (2013). Electronic banking and how courts approach to evidence. - *Computer Law and Security Review*, No 29, p 144.

[28] Porkess, R., Mason, S. (2012). Looking at debit and credit card fraud. – *Teaching Statistics*, Volume 34, Issue 3, p 87.

[29] Van Der Meulen, N. (2013). You've been warned: Consumer liability in Internet banking fraud – *Computer Law & Security Review*, Volume 29, Issue 6, p 717.

These days, the use of credit cards and other electronic payments, such as mobile and contactless payments, has become the most common and practical form of transactions.[30] This is because they are easy, fast, customer friendly and requires only a working internet connection and applicable devices, such as credit cards and smartphones, and they have achieved a strong position especially among educated and young people.[31] Unfortunately, this general way of fast-payments increases the possibility for misuse and fraud as the operative systems of service provider are not always guaranteed to prevent unauthorized use of devices, especially when the credit card or identification keys for online access are stolen.[32]

There are three usual banking-related issues where courts find it extremely hard to process electronic evidence, such as burden of proof, conflicts among the electronic evidence presented by the plaintiff and the defendant and the failure to reach balanced and acceptable decision for the matter.[33]

It is among common knowledge, that according to court practice the person who accuses another of some violation of another's rights, of wrong and harmful behavior or of any type of action has an obligation to prove his claims and allegations to be true and as opposite the party represented as a defendant is innocent, if not relevant and proper evidences are expressed and if there is no clear causal connection to the bearing issue. The purpose and idea of burden of proof is that during court proceedings or in some other dispute solving situation the event will start with a presumption of innocence towards the defendant whereas the plaintiff has burden of proof to prove his claims to be correct.[34]

---

[30] Koivunen, T., Tuorila, H. (2015). Consumer trust relations with payment cards and banks: an exploratory study. – *International Journal of Consumer Studies*, 39(2), p 85.

[31] Pulina, M. (2011). Consumer behavior in the credit card market: a banking case study. – *International journal of Consumer Studies*, Volume 35, Issue 1, p 87.

[32] Heikkinen, P., Iivarinen, T. (2011). Ensuring trust in electronic payment media. – *Journal of Payments Strategy & Systems,* Volume 5, Number 2, p 162.

[33] Mason (2013), *supra nota* 27, p 144.

[34] Douglas, W. (2014). *Burden of Proof, Presumption and Argumentation.* USA: Cambridge University Press. p 8

When disputes relate to banking, the bank must prove that it has exercised transactions under consumer's approval and therefore it must prove that transactions were verified by customer's signature.[35] For withdraws from ATM's or online transactions, the PIN code or online access keys proving the identity are valid signatures.[36] The Payment Services Directive for electronic payments and services on internal market area laid down by European Union was reformed on year 2018 and both the earlier and current version have similar regulation for use of the payment method provided by the bank, stating that the use itself is not a proof that the transaction was approved by the customer, that the customer behaved with neglect manners or failed on purpose or with gross negligence to fulfill one or more of the obligations placed upon him under article.[37] As opposite, the bank must prove that the transaction was approved and properly authenticated, recorded accurately and entered to records and that there were no other errors of defiance's on the function of operative system at the time of the payment, that could have led to corrupt recording or fraudulent payment in some other way.[38]

In Germany, the Federal Court reached an outcome in German case *Urteil vom 5. Oktober 2004 - Az. XI ZR 210/03*, stating that if person is not able to prove beyond reasonable doubt that his PIN code was not written on the card or stored in some other negligent way, he will be liable for damages because of negligent behavior against the terms of use of the contract that the ownership of the credit card requires.[39] The Court strongly based its decision on *prima facie* principle, which means that if some reasoning is not overpowered with relevant arguments and evidence, then it should be applied.[40] Person's credit card was stolen and used for cash withdrawal for total of 2000 DM. On final stage of the process, the Federal Court reached a decision stating that, because the plaintiff claimed that the card was not electronically read or

[35] Mason (2013), *supra nota* 27, p145.

[36] Ibid., p. 145.

[37] Mason, S., Bohm, N. (2017). Banking and fraud. – *Computer Law & Security Review*, Volume 33, Issue 2, p 239.

[38] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Accessible: http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm, 16 April 2018.

[39] Bundesgerichtshof [BGH], Urteil vom 5. Oktober 2004 - XI ZR 210/03

[40] Barcelo III, J.J. (2009). *Burden of Proof, Prima Facie Case and Presumption in WTO Dispute Settlement*. USA: Cornell Law Faculty Publications. p 42.

copied, the access to PIN and cash withdrawal by the third party cannot be based on nothing else but grossly negligent behavior of the plaintiff.[41] The Court also referred to law, which states that other events or happenings might have occurred, but as they cannot be proved or considered under common behavior they cannot be concluded.[42] As a conclusion, the client was accused for lying and acting against banks well-performing system, even though the bank was never demanded to prove the function of their system and its operational reliability but instead the court based its decision on arguments that the plaintiff could have written or stored the PIN with the card.[43]

To prove the correctness of its system, the bank must present evidence that the card was entered to ATM or point of sale terminals (POS) and that the legitimate user or a person authorized by him was using the credit card. The banks provide their system reports and summary of transactions as evidence to support their logic, containing a premise that if person's credit card was inserted to ATM with use of correct PIN, it means that customer's card was used by customer or another authorized person.[44] When the customer declines these claims, the bank provides stronger arguments by accusing the customer for being grossly negligent by not only making giving the card to the thief, but storing their PIN on the card in a way that it makes possible for thief to use both card and the PIN simultaneously.[45] Banks tend to forget the fact that the PIN can only be correct or incorrect, so no access to ATM is possible without using the correct PIN, so therefore assumed that consumer's duty to prevent the passing of PIN to third parties equals to grossly negligent behavior if theft has occurred.[46] By using this logic, the easy and possibility of stealing person's PIN by using of advanced technology methods with criminal intent is forgotten.

---

[41] Mason (2013), *supra nota* 27, p 147.

[42] Haybäck, G. (2009). Civil Law Liability for Unauthorized Withdrawals at ATMs in Germany. – *Digital Evidence and Electronic Signature Law Review*, Volume 6, p 64.

[43] *Ibid*., p. 64.

[44] *Ibid*., p. 57.

[45] Mason (2013), *supra nota* 27, p 145.

[46] Haybäck (2009), *supra nota* 42, p 59.

In addition, bank used an authored person as an expert witness to describe how it is nearly impossible to generate key that breaches the system algorithm or when considering the swift phases of theft and use of PIN, the PIN must have been able to be easily achieved by the thief. By these means the expert witness defended the view and the position of the bank.[47]

But even when expert witness is used, it does not mean that all the facts are presented or evaluated properly. One of the main priorities for banks is that consumers know how to safely use the payments and that the payment system itself is working, because these are essential functions on banking daily basis.[48] It is interesting that the court did not require the bank to demonstrate the function of their system and the decision of the Federal Court seemed to be straightforward without any significant comment, value or thought given to the plaintiff.

The duties and obligations of both parties should always not only be presented in accordance with the law but also tested, meaning that the given evidence is not only theoretical but representing truth while negligence and intent being evaluated at the same time. In jurisprudence, intent contains negligence and cause, even that separation of those two is not needed in matters relating to compensation of damages.[49] Intent does not have clear explanations or features but it should be always evaluated on case-by-case basis.[50]

Both customer and card issuer must be aware of the negative consequences followed by a wrongful use of credit card, but especially the latter, because the banks are strictly regulated by laws, treaties and other regulation. When customer has received his credit card, he must accept the use of bank's technology and this way trusts that bank supervision and security measures prevent any fraudulent action directed to him. Phishing, credit card copying, malware installations to ATMs and hacking of bank information in addition to theft are modern ways of

[47] Mason (2013), *supra nota* 27, p 146.

[48] Pavia, J. M., Veres-Ferrer, E. J. (2016). Is the cardholder an efficient alarm system to detect credit card incidents? – *International Journal of Consumer Studies,* Volume 40, Issue 2, p 230.

[49] Hahto, V. (2008). *Tuottamus vahingonkorvausoikeudessa*. Finland: Talentum Media. p 104.

[50] *Ibid*., p 104

illegal access to payment devices and they happen relatively often[51] This way banks are forcing customers to rely on technology that is not perfect and correspondingly accuse customers for being neglect.[52]

United States vs. Albert Gonzalez provides an overview to weakness of bank systems, as Gonzalez and his companion launched unauthorized access on databases storing credit and debit card transactions and stole encrypted PIN data for over 130 million credit and debit cards.[53] Even that such activity requires professionalism and criminal intent, the case proves that banks do not always have most efficient security systems, but dysfunctions are present.

In Norway has occurred two relevant cases, which give depth analysis that the courts do not question evidence given by the bank, value the evidentiary claims presented by the opposite party or accept alternative explanations but instead rely that standards of bank security system are effective.[54] The courts have accepted bank data as evidence without knowing whether it were valid, contained errors that were not realized or even handled appropriately by qualified personnel and have ended up with a decision that there were no reason to believe for existence of errors in bank's security system.[55]

On case *Bernt Petter Jørgensen v DnB NOR Bank ASA,* a dispute raised after person's credit card was stolen and unauthorized payment transactions were conducted soon after the theft.[56] According to Norwegian legislation, the court required the bank to prove the gross negligent actions of the plaintiff, but because encryption or guessing a correct PIN is considered to be almost impossible the court ended up with a decision that the person has acted with gross

---

[51] https://www.statista.com/statistics/326169/united-kingdom-uk-online-banking-losses/, Accessibe 15 April 2018.

[52] Mason, S. (2012). Debit cards, ATMs and negligence of the bank and customer. – *Butterworths Journal of International Banking and Financial Law*, Volume 27, Number 3, p 167.

[53] Court Decision, *United States vs. Albert Gonzalez.* United States Court of Appeals, First Circuit. NO. 00-1598. October 11, 2001.

[54] Nuth, M.S. (2012). Unauthorized Use of Bank Cards with or without the PIN: A Lost Case for the Customer?. – *Digital Evidence and Electronic Signature Law Review*, Volume 9, p 98.

[55] Mason (2013), *supra nota* 27, p 147.

[56] *Ibid.*, p. 147.

negligence.[57] The court made several mistakes as it did not have evidence that the card or PIN were shared to third parties or stored with negligence, did not require bank to prove otherwise or question any data presented by the bank and based its decision on evidence that it not sufficient in terms of law.[58] Therefore, it can be noted that the court made mistakes by abstaining from ensuring the quality and feature of electronic evidence as well as for making assumptions based on evidence that is not distinct.

The case of *Pål-Gunnar Øiestad* demonstrates that the court may shift the burden of proof towards weaker party without evidence suggesting doing so.[59] Øiestad's family had three Mastercard cards and one of them was stolen in Rome and used for transactions over 50,000 NOK before cancelling of the card.[60] Øiestad claimed that PIN were not written to any of the cards because it was on memory, but bank accused him of gross negligence on basis of storing code with the stolen card, making it possible for thief to perform transactions.[61] The bank did not present any evidence that code and the card were stored together and court decided the case on favor of the bank, although giving Øiestad a permission to appeal.[62] Before proceedings on Court of Appeal, the bank sent a letter to Øiestad stating that no transactions were made by using the PIN and admitted to compensate every damage Øiestad and his family had suffered.[63]

On these cases, the court should have at least required the bank to provide evidence that the PIN was used, require reliable data that both card and the PIN were stored together and not accept low standard evidence from the bank instead of making decisions without properly testing evidence and claims of both parties.[64] It must emphasized that even though the decisions did lack proof of authentic evidence, the court processed with prudence as banks do offer highest security

---

[57] Nuth (2012), *supra nota* 54, p 96.

[58] *Ibid.*, p. 97.

[59] Mason (2013), *supra nota* 27, p 147.

[60] Nuth (2012), *supra nota* 54, p 98.

[61] *Ibid*, p. 98.

[62] *Ibid*, p. 99.

[63] *Ibid*, p. 98.

[64] *Ibid*, p 99.

level of credit cards and it is easy to rely on them.[65] It is just that no relying should happen with passing off the evidence or reasonable doubts.

1.2.1. AN EXEMPLARY INTERPRETATION

On case *Z.S v Lietuvos taupomasis bankas,* the Supreme Court of Lithuania processed the case with appropriate means and emphasized the liabilities of banks in situation where the weaker party has suffered damages because of failure of professionalism and lack of care of more powerful party. The plaintiff (*Z.S)* deposited 800 Litas on 26th of August 1999 and 48,200 Litas on the following day to his bank account and on 29th of August plaintiff was informed that nearly all the money was withdrawn from several ATMs in Poland.[66] The plaintiff claimed that he had not authorized such actions and the bank refused to provide compensation, based on allegations of negligence and lack of following duty of care with the card.[67] Vilnius 2nd District court declined plaintiff's claim for compensation on basis that there were no lack of diligence, faults or careless on defendant's activity, but the Supreme Court changed the decision later on. Supreme Court required bank to cover damages and other cost after finding out that at the same time when transactions were made in Poland, the card was used by the plaintiff in Lithuania, which indicated fraud and unauthorized access on credit card.[68]

The Supreme Court gave three crucial statements on its outcome, firstly that banks are specialized financial institution required to operate with credibility, safety and trust and by using their services the client may expect the requirements to be fulfilled on every basis. When client suffers damages because of failure of ensuring credibility, safety and trust or lack of diligence and care, the bank may be considered liable. The payment card transactions also fall into the scope of banks professional activity and because of that bank must ensure the security and functionality of the card, meaning that if client has not been grossly negligent it will bear risks of

[65] *Ibid,* p 98.

[66] Mason (2013), *supra nota* 27, p 147.

[67] Mason (2013), *supra nota* 27, p 148.

[68] *Ibid*., p. 148.

fraudulent activity.[69] Some legislations favor procedure where reasonable likelihood of presented evidence is enough for the court to decide.[70] As courts are obliged to provide decision and arguments for the case based on all given evidence and circumstances, issues may arise when electronic evidence is addressed poorly. [71]

[69] *Ibid*., p. 148.

[70] Lappalainen, J. (2001). *Siviiliprosessioikeus*. Finland: Talentum Media Oy. p 307.

[71]Tapanila, A. (2007). *Tuomarin esteellisyys.* Finland: Suomalainen Lakimiesyhdistys. p 41.

2. THE COURT PROCEEDINGS ON ELECTRONIC EVIDENCE IN FINLAND

The court has the duty to rule the course of the legal proceedings and to make sure that all steps are treated with appropriate legal customs.[72] Its purpose is to strengthen the national legislation and guarantee fundamental rights, such as right to fair trial and no punishment without law, derived from articles 6 and 7 of European Convention of Human Rights and §21 from the Constitution of Finland.

2.1. The fundamental evidentiary rules in Finnish legislation

Code of Judicial Procedure (hereinafter CJP) regulates civil procedures in Finland and its chapter 17 contain fundamental rules for law on evidence. Documentary evidence, witnesses, expert witnesses, judicial inspection and hearing are approved types of evidence recognized and do not require minimum standards, except that evidence obtained by torture or by illegal methods will not be admitted for proceeding.[73] Duty to provide evidence and the burden to proof own claims to be true may shift to opposite party if another party supports his claim with sufficient statements.[74] In that case an obligation to object the claims is imposed on another party member. [75]

The reason why there are no evidentiary requirements for is because of two fundamental principles governing the law on evidence, free assessment and free disposition of evidence.[76] Free assessment means that the court must include every presented evidence and details of the case without compulsory and binding rules regulating the evidentiary value in advance. [77]

---

[72] Code of Judicial Procedure 1.1.1734/4. §6

[73] Koulu (2015), *supra nota* 1, p 14.

[74] Lappalainen (2001), *supra nota* 70, p 307.

[75] *Ibid.*, p 307.

[76] *Ibid.*, p 139

[77] *Ibid.*, p 138

Chapter 17 paragraph 2 on CJP further on states that methods of collecting evidence are not restricted in any way, unless they question the reliability of evidence, for example for being unnecessary, obtained illegally, replaceable or beyond reach.[78] In the other hand, the court is bound by the claims and statements of the parties, meaning that it may not seek evidence or details of occurred events by itself but has to consider situation on with care and case-by-case basis and declare the judgement.[79] For electronic evidence this would mean that the court must examine the causal relation of given or questioned electronic evidence and claims of the parties and to reach an outcome without favoring another.[80] The causal relation may be used as main argument of the court decision, even when that it does not stand for the full truth but for reasonable likelihood of precision for claims of the parties.[81] The standards of evidence are extended to cover electronic evidence while the treatment, admissibility and reliability of evidence are determined and evaluated by court but no common knowledge is required to be proven.[82] Court has power to use expert witnesses or professional in when lack of knowledge or understanding of electronic evidence.[83] There are no best evidence rule used in legislation or in practice.[84]

Certain standard requirements of evidence must be fulfilled, such as being lawfully obtained and relevant, but the last decision is always made by the judge[85]. Judge may reject the evidence in use of court proceedings even if all the features of evidence are suitable, but it lacks element, such as not a clear connection to the matter or shady aspects, leading to a situation where the doubt remains.[86] The court will give an overall evaluation on authenticity of evidence and if it can be used in the court process and when evidence is admitted, it can be used to give power and

[78] CPJ, *supra nota* 72, §17: 2.

[79] Koulu (2015), *supra nota* 1, p 2.

[80] Hemmo, M. (2005). *Vahingonkorvausoikeus*. Porvoo: WS Bookwell Oy. p 125

[81] *Ibid*., p 125

[82] Lappalainen (2001), *supra nota* 70, p 145.

[83] Koulu (2015), *supra nota 1*, p 17.

[84] Ibid., p. 17.

[85] Ibid., p. 14.

[86] Hallberg, P. (2001). *Oikeudenmukainen oikeudenkäynti 2000-luvulla.* Finland: Talentum Media. p 72

reliability to the processed case.[87] The court must present grounds for assessing evidence in its decision.[88] Usually in jurisprudence the level of proof that is enough to convince the judge is referred to by words "presumable", "probable", "evident" or "definite" as in practice "sensible preponderance of evidence" is considered to fulfil the burden of proof.[89] This refers to a general practice of proving something "beyond reasonable doubt" Besides these formulations of provisions, there are no minimum standard of proof to consider a fact as establish in Finnish procedural law.[90]

In Finnish civil procedure, there are no means of evidence which would be excluded from possible modes of proof. This is considered to follow from free assessment of evidence. However, there is a rule that evidence on notorious facts or facts that the court knows need not be proven.[91] The electronic evidence is far more often excluded in criminal court than in civil court if the terms are not fulfilled, because the civil court matters tend to be more straightforward and have less substantial impact in form of sanctions.[92].

The court will give an overall evaluation on authenticity of evidence and if it can be used in the court process. It must be analyzed that should it be a mandatory to challenge the authenticity of the electronic evidence in court or should there be a general phase for authenticity of such evidences be proven on court proceedings, without additional questioning from another party.[93] Such action forces the court to evaluate the authenticity of given single evidence or in more demanding proceeding all aspect of given evidence may be challenged.[94]

---

[87] Lappalainen (2001), *supra nota* 70, p 294.

[88] Lappalainen (2001), *supra nota* 70, p 294.

[89] Koulu (2015), *supra nota* 1, p 13.

[90] Koulu (2015), *supra nota* 1, p 10.

[91] Lappalainen (2001), *supra nota* 70, 145.

[92] *Ibid*., p 346.

[93] *Ibid*., p 346.

[94] Virolainen, J., Martikainen, P. (2010). *Tuomion perusteleminen.* Finland: Alma Talent. p 295

There are of course situations where the original source of evidence cannot be approached, presented or examined, because it is in unreadable form or destroyed completely. A partly destructed evidence could be admitted, because it still contains the relevant data, but if the copy of it does contain the overall description of the matter without degrading effect on reliability of evidence, it should be prioritized.[95] As mentioned before, the court will make a decision whether or not the evidence is accepted or if there are heavy reasons for dismissal of evidence[96] Free dispositive of parties means that in Finnish legislative system there is a different treatment on dispositive and non-dispositive cases. Dispositive cases may be settled in any occasion, but on non-dispositive cases the court will make the decision or provide guidelines as settlement rarely is accepted.[97] Free disposition of parties also means that a possibility to be heard and give statements must be given to both parties.[98] During process of non-dispositive cases the court has an exception on rule of treatment of evidence[99], as it may collect evidence on its own if such actions do not directly or indirectly worse the position of the defendant.[100]

The court members are as well prohibited of using knowledge and details relating to processed case that they have acquired outside of the court process. Such information must come through procedural affairs during trial.[101] Evidence cannot be represented on preliminary stage of court proceedings unless there are relevant reasons why the evidence was not able to be presented in the first place but instead it should be always presented in a way that a person whom has no more than basic knowledge of the area that the evidence represents is able to understand the matter with no lack of details and chance to present the evidence cannot be denied without serious justifications.[102]According to Finnish law, for person to be ruled on grounds of negligence or

[95] CPJ, *supra nota* 72, §17: 2, 25.

[96] Lappalainen (2001), *supra nota* 70, p 138.

[97] Koulu (2015), *supra nota* 1, p 2

[98] Niemi, J. (2010). *Civil Procedure in Finland.* Netherlands: Kluwer Law International BV p 79.

[99] CPJ, *supra nota* 72, 24 § 4.

[100] Koulu (2015), *supra nota* 1, p 20

[101] Lappalainen (2001), *supra nota* 70, 141.

[102] Leroux, O. (2007). Legal Admissibility of Evidence. – *International Review of Law, Computers & Technology*, Volume 18, Issue 2, p 194.

grossly negligent behavior, it must be proved that person has acted with intent or knowingly.[103] Negligence has a significant impact on some of the following cases.

2.2. Questionable approach for unauthorized access on payment services in Finnish case-law

On the Finnish legislation the Payment Services Act (hereinafter PSA) represents the modern EU legislation of electronic payments and its chapter §62 defines the liabilities and limitations of the user on situation of unauthorized access while §63 state the liabilities of the payment service provider.[104]

According to §62 of the Act, a person is liable for unauthorized use of the payment device if:

1. *"he or she has passed it someone else and given an authorization to use it,*
2. *lost, theft or unauthorized access has happened because of neglect behavior of the user,*
3. *legitimate owner or authorized user at the time has not informed the service provider or person addressed by it of the lost, theft or unauthorized access of the payment device."*[105]

The person will not be responsible for unauthorized access when information on paragraph 3 has been made or if service provider's actions have prevented the possibility of doing such information.[106] It must be clarified that the scope of term "payment device" can be extended to cover electronic payments, such as typical online bank transactions or other fast-payment methods.[107]

The service provider will be considered liable for unauthorized access and obliged to restore the financial status of the client, when a payment transaction has happened unlawfully, and

[103] Hahto (2008), *supra nota* 49, p 108

[104] MaksupalveluLaki. 30.4.2010/290. PSA.

[105] *Ibid,* §62, points 2-4.

[106] *Ibid,* §62, points 7-10.

[107] PSA, *supra nota* 104, §8.

exceptions provided on chapter §62 do not apply on the situation.[108] When liabilities of §62 and §63 are evaluated, they can be considered to have following three levels; rightful behavior and authorized transaction that make consumer free of payback liabilities, neglect behavior constituting personal risk damages on 50 euros at the most if they do not have feature of gross negligence and that gross negligent behavior equals for having a full responsibility for covering the damages on the matter.[109] The client must also take all reasonable steps to follow the terms and conditions of the banks.

During these modern times during the era of technology, the avoidance of use or interaction of technology is really hard or even impossible, so lawyers must have an excellent understanding on technological matters inside the field of law and be aware of the operational commands and obligations that arise in case when there has happened an unfavorable occasion.[110] The burden of proof has more wide and specific meaning when electronic evidence is addressed, because informative data used as evidence can be in many different forms while some of them can be extremely hard to explore, they are endangered for modification or deletion, they can be hard to find and even more difficult to be assigned as admissible on court, because some of them can easily be overpowered if there is a lack of some fundamental feature of evidence.[111]

The value of burden of proof and the weight it carries can be observed and understood from court procedures relating to online banking disputes and issues between credit card holder and payment service provider. But what happens when the situation does not proceed in a way that we think it would under normal conditions? The consumer protection and rights and regulations regarding to it do not always guarantee an outcome for the consumer and as banks tend to achieve the most favorable outcome for them, so there is a chance that banks or financial institutions are shifting the burden of proof in a way that the consumer is placed under extremely

---

[108] PSA, *supra nota* 104, §63.

[109] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Accessible: http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm, 16 April 2018.

[110] Mason (2013), *supra nota* 27, p 149.

[111] Hock, L.H. (2008). *A Philosophy of Evidence Law: Justice in the Search for Truth*. New York: Oxford University Press Inc. p 163.

difficult position. By shifting the burden of proof, a party may protect its own position and obtain a position where its claim is presumed to be the right one for the situation.[112] A presumption of claimed happenings is not sufficient reason for decision but facts and happenings of the situation should be at least tried to be presented as accurate as possible.[113]

The above-mentioned chapters §62 and §63 of Payment Services Act and general obligations of parties to prove at court mean that banks must prove the following:

- The payment transaction was valid, leaving no chance of errors during the payment process.
- The payment was recorded on bank's system
- There were no other errors of defiance's on the function of operative system at the time of the payment, that could have led to corrupt recording or fraudulent payment in some other way.[114]

Courts should always require the banks or other payment service providers to prove these elements to support their case, before relying on their behalf and shifting the burden of proof towards other party.

The situation can be demonstrated by decision *KKO: 2006:81* of Finnish Supreme Court. In that case the bank (Nordea) had granted a MasterCard Gold credit card to client which was stolen during his business trip on Spain and afterwards used to purchase in total of 21 different transactions.[115] The sellers had checked the card under rules that oblige them to confirm whether card is stolen or out of service. Nordea claimed a sum of 2870,18 euros for damages from the client, which he paid but filed a lawsuit later for refund. Person stated that according to chapter 7 §19 of Consumer Protection law at the time he was not liable those transactions as he had kept the card within his reach and was aware of the whereabouts of the card all the time and his behavior was not negligent or increase the possibility of theft. He had kept his wallet in his

---

[112] Räikkä, J. (2005). Global Justice and the Logic of the Burden of Proof. – *Metaphilosophy*. Volume 36, Issue 1-2, p 228.

[113] Plumer, G. (2017). Presumptions, Assumptions and Presuppositions of Ordinary Arguments. – *Argumentation*, Volume 31, Issue 3, p 475.

[114] Mason (2013), *supra nota* 27, p 145.

[115] Korkein Oikeus, KKO:2006:81, 16.10.2006, point 3.

pocket, had not used his own money on business trip, had kept doors locked during night and the persons he travelled with confirmed that no extraordinary situations happened that could be reasons for the theft. Nordea called him and informed of attempt of access to his credit card on ATM and at this time he requested Nordea to shut down the card.[116]

Person also stated that terms of use did not oblige him to store credit card with special security methods in daily basics, whether he was abroad or not. Nordea stated that the person had been negligent, behaved with irresponsible manners and failed to follow higher duty of care, which requires person to take extremely good care of his belongings while abroad. Higher duty of care was not mentioned in terms of contract and there were no contractual legal requirements for the card owner to check presence of his card daily or within certain time frame. Nordea objected the claim and requested that they should not provide any refund.[117]

Both lower courts dismissed person's claim and found his that his behavior has been negligent, because person had not secured his credit card with appropriate measures all the time in situation where the possibility of theft is higher, meaning that thieves are well-known to favor places of crowd masses and tourist areas. The Supreme Court upheld the ruling of lower courts and stated that as there is even a slight chance for negligent behavior, person is responsible for illegal use of the credit card and have no obligation to receive compensation for the damages from Nordea.[118]

The chapter 7 §19 of Consumer Protection law had similar regulation for freedom of responsibilities currently regulated by Payment Services Act §62. §62 regulates that a person who has lost the possession of his card without neglect behavior is responsible for unauthorized access or illegal use only if he did not inform the service provider about the loss or theft of the card. The problem that arises is that the courts did not examine the terms of contract or even demand Nordea to provide sufficient proof to support their claims, but instead relied on statements of Nordea and did not examine that whether the disputed duty of higher care really did exist. Especially the Supreme Court should have taken a different approach and analyze was

[116] *Ibid*., point 4.

[117] *Ibid.*, points 10-12.

[118] *Ibid.,* points 35-36.

person's behavior negligent at all. The Courts indirectly favored statements of Nordea without giving overview to all details and aspects that may stand for facts of the case.

The case *KKO: 2006:81* and its decision does not give clear understanding of possible shifts of burden of proof, but it has a causal link for next two cases, where the operating bank system occurs an error on identification of client and causes damages to client without possibility of proving his actions while same time placing him on unfavorable position.

Finnish Financial Ombudsman Bureau (Fine) is an institute which provides legal decisions and recommendations for dispute situations relating to all financial and consumer protection issues. Fine also co-operates and observes activity of banks or other financial authorities and law enforcement has recognized and accepted its formal guidelines for fraudulent use and reporting of misuse of payment card, which are in clear balance with the regulating laws and acts.[119]

On Fine case *PKL 77/11* person's credit card was stolen and unauthorized transactions were made frequently within short time period.[120] Because all transactions were authorized by PIN, Fine considered that it is impossible that the theft could have obtained the PIN and came into conclusion that only possible option is that person has stored both card and PIN together and made it possible for theft to instantly use the card after obtaining it. Fine stated that person has been grossly negligent and is liable for all harm caused by those unauthorized transactions.[121] Person provided evidence proving that he the last time he used the card was over twelve hours ago in a place far away from the place where the theft had occurred. Fine noticed that even person gave evidence of actual happenings, he is not able to give detailed explanation how the card ended up being stolen. With these grounds Fine upheld its decision that only possible option

[119] Korttiturvallisuus. (2012) Shared Guidelines for Using Payment Cards. [Online] https://www.korttiturvallisuus.fi/en/Help/Reporting-misuse/ 12. March2018

[120] The Finnish Financial Ombudsman of Bureau (FINE). Ruling: PKL 77/11, point 1. Accessible: https://www.fine.fi/ratkaisutietokannat/ratkaisu/pkl-7711.html, 12 March 2018.

[121] *Ibid*, point 17.

for theft is that PIN and card were stored simultaneously, and so person will carry the full responsibility.[122]

On Fine case *75/11* person's stolen credit card was used to make multiple unauthorized withdraws from ATM by entering a correct PIN code.[123] A same interpretation was used than in *77/11* as Fine found out that only logical explanation is grossly negligent behavior because the PIN and card were stored in the same place.[124] No evidence was presented, or claims given that would indicate or verify such explanation to be true. Fine also stated that because the cardholder had used last time himself the card on earlier day, it is not possible that the theft was able to obtain the PIN. Person counterclaimed with facts that the card was taken from her purse when she was on a tram and when she had found out that the card was missing she thought she had left it at home. Three hours later she shut down the card, but Fine stated that three hours is too long delay and equal to lack of duty to take care, so her behavior has been negligent, and she is fully liable for the occurred damages.[125]

The time-limit based grounds are suspicious and in conflict with Fine case *4/12* which defined what can be considered as delayed information of loss of credit card and ruled that if person has informed about the loss within five hours he or she has acted with good faith and care.[126] There is clearly a distinct interpretation between the decisions based on time frames even that they have been given by the same official. Fine failed to use proper interpretation and shifted its standards when it should have followed similar proceeding and grounds for judgement made by itself earlier. When an official authority does not follow the guidelines it has created itself and gives a different ruling on similar matter, the trust towards it decreases significantly.

---

[122] *Ibid*, point 23.

[123] The Finnish Financial Ombudsman of Bureau (FINE). Ruling: PKL 75/11, point 1. Accessible: https://www.fine.fi/ratkaisutietokannat/ratkaisu/pkl-7511.html , 12 March 2018.

[124] *Ibid.*, point 6.

[125] *Ibid.*, point 7.

[126] The Finnish Financial Ombudsman of Bureau (FINE). Ruling: PKL 4/12, points 30,33. Accessible: https://www.fine.fi/ratkaisutietokannat/ratkaisu/pkl-412.html 14 March 2018.

The EU Directive 1999/93/EC of Community framework for electronic signatures was imposed to Finnish legislation by the Law on Strong Electronic Authentication and Electronic Signatures (EIA)[127] and chapter on its modern version 2§17 requires that electronic identification by user is proceeded with official documents or by certain type of access keys, given by the service provider.[128]The Payment Services Act contains similar content and chapter 63§ of the Act states that the service provider must cover the expenses and return the amount to the client when it has been informed or has found out that such event has occurred. If there is evidence or even a doubt of fraudulent action on client behalf, the service provider must declare a written statement and deliver it to Financial Supervisory Authority.[129]

As discussed above, the legitimate user of the credit may be liable for unauthorized transactions of the credit card, if he has given the card to someone else, showed negligence against terms of use of the contract or have failed to inform the unauthorized use of the payment device.[130] The Payment Services Act also states that the service provider does have a higher responsibility of taking care of the operating system and has an obligation to ensure its function, prevent access from any third-party personnel and the terms and conditions given by the service provider must not be unjustified or discriminatory[131]

On case *KKO: 1994:82*, Mr. Niskanen filed a lawsuit against Diners Club Finland (DC) and claimed back 38,000 Finnish marks that were taken from his card after it was stolen.[132] Under Supreme Court's evaluation, it was undisputed fact between parties that the client had shown negligence on his duty to inform from loss, misuse or theft the service provider right away after discovery such as the DC was notified two days after the theft. The event under dispute was the approval of transactions through sellers as third-party confirmers and as the banks have systems

---

[127] Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. – *Identity in the Information Society*, Volume 3, Issue 1, p 182.

[128]Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 29.06.2016/533. EIA.

[129] PSA, *supra nota* 104, §83, points 2-4.

[130] Hahto (2008), *supra nota* 49, p 100.

[131] PSA, *supra nota* 104, §82 a-c.

[132] Korkein Oikeus, KKO: 1994:82, 8.9.1994. points 1-3.

for verifications of payments for uncommon amounts why DC did not have such quality.[133] According to DC protocol, identity was required to verify through DC by phone for unusual amounts.[134] Several transactions between 1,100 and 10200 marks were approved by only looking at signature on receipt and in card.[135]

The Supreme Court stated that by phone call verification the transaction would not be prevented, because the person had failed to inform the card stolen, but such phone call in addition to other security measures might have given a reason for DC to doubt a misuse and contact their client. In that case further illegal transactions would have been prevented and both parties would instantly have been aware of the theft. Based on these evidentiary statements, the Supreme Court held Mr. Niskanen liable for occurred damages plus all expenses. The court based its decision on law on consumer protection of that time, which stated that the seller's liability to verify transactions must be evaluated, not based on certain details, such as sum or features of the buyer and to facts that happenings abroad are hard to prove, and the unlimited credit of the card may expose to situation where uncommon transactions do happen.[136]

When evaluating this case, the person's failure on duty to inform or amount of damages he had to pay to DC are not relevant, but instead should be notified that even that the court agreed that a phone call could have made a difference, it did not require DC to prove that there was no defiance on its operating system that could have blocked the call. The court also did not question did DC have any additional security measures relating to use of unlimited credit card and why there were no back-up measures to prevent transactions above 3000 marks if phone call was not made. According to paragraph 19§ of modern Payment Institutions Act, the service provider offering payment services must by all means and methods preserve the function of their operating system and create efficient surveillance system to control the possible risks.[137] The law on consumer protection on time when the decision was made, stated that the owner of the credit card is not liable of unauthorized use of the card regardless of negligence on informing the loss

[133] *Ibid.,* points 24, 29.

[134] *Ibid.,* points 27-28.

[135] *Ibid*, point 27.

[136] i*bid*, points 31, 50-52.

[137] PSA, *supra nota* 104, §19.

of it, if the seller has failed to verify the third party's right to use the card[138] Custom is directly not applicable in such situation but gives thoughts on that different approaches and interpretations could be made. A trust into operative procedures and customer-relationships of banking and other similar services may lower significantly on customer's behalf in addition to financial losses.[139]

2.3. Correct approach on unauthorized access on payment services in Finnish case-law

KouHo: 2012:3 refers to a case where person's spouse had used his online banking password and identification documents to increase the credit limit of his credit card online, transferred money to shared bank account and used them for her own purposes.[140] Unauthorized use continued for over two years before person found out about the actions of his spouse. According to the bank person was neglect and his actions were irresponsible, because the password and identification documents for the use of operating online system of the bank should have kept efficiently apart from each other, in a way that not even a family member is able to use them or aware of their location.[141] Undisputed matter between parties was the fact that person could have easily found out his account activity by verifying it occasionally, even that in Finnish law there is no direct command or statutory obligation to check account balance or search for fraudulent activity to ensure that no misuse have happened within certain time limit, but it is under common knowledge that person should have an overview of his or her financial status.[142]

The District Court first stated that bank is to be held liable for damages as even that access and identification keys are required to be secured from any outsider, a spouse can not be considered as one, so person had stored them carefully enough. The Court of Appeal reversed the lower

---

[138] KKO: 1994:82, *supra note* 132, points 24-25.

[139] Hoffmann, A.O.I., Birnbirch, C. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. – *International journal of Bank Marketing*, Vol 30, Issue 5, p 392.

[140] Kouvolan Hovioikeus, *KouHo:2012:3*, 5.1.2012, point 1.

[141] Kouvolan Hovioikeus, *KouHo:2012:3*, 5.1.2012, point 3.

[142] *Ibid*., points 34-35.

court's decision and gave more value to the position of the bank, on basis that because spouse had already huge financial difficulties and was used to spent money over her limits the cardholder had presented grossly negligent behavior when lacking to verify account balance for over two years.[143] The cardholder was considered to be fully liable for his passive behavior and of her fraudulent actions and at same time the Court of Appeal created a precedence which defines that if the cardholder does not notice unauthorized access of his card for many years, he has been grossly negligent.

The court showed good interpretation of law on assessment of claims of parties and addressed to what extent person's passive behavior transforms to grossly negligent behavior on case when he has no idea of fraudulent actions on his credit card in the first place. The court used force of law efficiently when it was able to provide a ruling on matter where person followed standard requirements by instantly informing about the unauthorized use but had not done anything about it when he easily could have affected the happenings earlier.

The District Court of Helsinki gave ruling for case *HelHO: 2007:2,* where person filed a lawsuit against bank Nordea, because his credit card was stolen when he was at hospital and used for unauthorized payments for several times.[144]The person informed about the loss of card after a month of those transactions because he was then released from the hospital. Over 3000 euros was stolen, and the seller had verified that the card was not stolen and confirmed that everything else was convincing as well. The bank (Nordea) stated that person had not followed his duty of care as he informed with long delay and because the seller had acted with responsibility, the person should be liable for damages on basis of negligence. Nordea provided evidence of approved transactions and referred to case judgement of *KKO: 1994:82,* which stated that the seller must verify identity of person using the card only when there are special reasons to believe of fraudulent use.[145] The court dismissed Nordea's evidence and ruled in favor of the plaintiff.

[143] *Ibid*., points 50, 65-66.

[144] Helsingin Hovioikeus, HelHO: 2007:2. The Court of Appeal of Helsinki, point 2.

[145] *Ibid*., point 24.

The Court of Appeal of Helsinki did not change the outcome of lower court, but highlighted that extraordinary circumstances, such as recovery at hospital on time of theft, does not fall on scope of negligence as it would be unreasonable.[146]

As stated earlier, The Payment Services Act 53§ legislates for negligence of legitimate owner of the payment device with statements that oblige him to use payment device under the terms and conditions given by service provider since the person has received them, take care of the device and passwords with reasonable methods while the service provider must make sure that no one else have possible access to password or similar access keys. The last section means that the service provider must by all means make sure that unauthorized use of the payment device would be extremely hard or impossible, which first off means that they must keep such data secure themselves and second they must make sure that the operating online system does work properly. Correct authentication, passwords / PINs, signatures, recordings and any technical failure are regarded to be part of the operating online system and belong to the area of evidence which the bank must be able to prove if questioned.[147] The duty to take care should be approached with overall estimate, instead of evaluating each circumstance, while chances of damages and avoidance should be taken into consideration.[148]

[146] *Ibid*., point 54-55.

[147] Mason (2013), *supra nota* 27, p 145.

[148] Hallberg (2001), *supra nota* 86, p 72.

3. ALTERNATIVE OPTIONS FOR REINFORCING THE LACKING CUSTOMS OF COURTS ON PROCESS OF ELECTRONIC EVIDENCE

Courts have many underlying problems on processing of electronic evidence that derive from lack of knowledge, incompetency, unfamiliar subject or expertise or from incorrect approach and interpretation to the legal matter. When courts do not have complete understanding for the processed case, they might easily rely on claims and evidence presented by bank or authority and same time indirectly dismiss or decrease the arguments of the other party. As described with case law above, such behavior will lead to favoring one party on expense of another's judicial rights. There are several alternative means, some easy and some very hard to implement, that would provide tools for more designated, applicable and as most important more judicial interpretation and ruling for courts.

More precise and wider understanding of new technology is needed on process of electronic evidence, as courts already have admitted malicious and unreliable data as evidence not because they committed something wrong, but because they did not have sufficient knowledge or understanding to examine the authenticity of the evidence.[149] As the number of electronic evidence will grow inevitably, the courts must understand and question the idea that computers work correctly and produce flawless evidence.[150] The significant growth of electronic evidence obliges law makers to develop a legislation that would be neutral and cover protection under the law to all parties.[151] Legislation should not be too loose, because it would lead to straightforward, inaccurate and unilateral interpretation of law and if the legislation is created to be too strict, problems will occur as well, such as unnecessary limitations for innovations and for certain electronic payments and these would together slow down the technological development of the society. Therefore, it is important for the legislation to be strict and detailed enough to

[149] Thomson (2013), *supra nota* 10, p 5.

[150] Mason (2017), *supra nota* 2, p 240.

[151] Daniel, L, E., Daniel, L.E. (2011). *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*. 1st Ed. USA: Elsevier. p 52.

cover the rights of all parties but at the same time to make room for things to evolve and maintain security.

The role of the judges in courts is crucial as they are the ones applying legal force and analyzing evidence. Because the possibilities to manipulate electronic evidence are endless, the judges should be up to date of latest technology, practice, function and differ the capabilities that electronic data may represent.[152] Instead of assigning the evidence instantly under analysis and determination of judge, we should focus define the effort judges have made to be qualified for give decision for the matter.[153] One significant problem is court's responsibility for use of expert witnesses, like they did on case *Urteil vom 5. Oktober 2004 - Az. XI ZR 210/03* to strengthen banks statements. The issue is that, if a judge lacks knowledge, understanding or is in some other way incompatible to provide arguments to the case without addressing expert witness or professional, in that case who has the authority to guarantee that the expert knows his matter completely or if he provides incorrect information and court relies on that, we instantly have misleading evidence giving effect on court. The judge cannot know beforehand the credibility or content of expert witnesses, so the judge must consider the testimony of expert witnesses or professionals carefully.[154]

Having judges with practical expertise to the addressed matter will eventually decrease occasional shifting of burden of proof and reduce situations where courts trust statements of one party only because it is an institutional authority that cannot be false. Case *Jørgensen* proved what may happen when members of court do have sufficient understanding of electronic evidence and how lightly they may shift the burden of proof while treating the evidence of the claimant with lower dignity. Fine cases *77 /11* and *4/12* demonstrate unequal treatment of claimant and strange interpretation of law, as Fine showed no interest towards its own earlier ruling. The Lithuanian case instead proved that court members with excellent understanding and knowledge of electronic evidence can provide an excellent ruling, and not to value status but instead the content of evidence.

---

[152] Thomson (2013), *supra nota* 10, p 1.

[153] Tapanila (2007), *supra nota* 71, p 48.

[154] Lappalainen (2001), *supra nota* 70, p 475.

There should be expert arbitration committee analyzing electronic evidence as alternative to courts instead of decisions ruled by old judges with insufficient expertise for obtaining fully understanding. Eventually electronic evidence will cover all or at least most of the courts materials and then the responsibility of courts as users of law will be significantly higher. Tests that verify understanding to modern evidentiary aspects of technology could be used to ensure the qualification of judges. In addition, there could be tests like bar exams or doctoral dissertation that would provide certificates of different levels for the person that would be needed to update within certain time. This would be one way to ensure that on there would always be qualified professionals on court. On another hand, such educational system would have to be worldwide and cover all the same aspect, otherwise a possibility for loopholes and different legislations would create distinct legal customs. Professional European framework could advice law enforcement, legal authorities and police for more proper treatment of electronic evidence, so that altered or corrupt evidence would not proceed all the way to court but could be identified earlier. The remaining task for court would then balancing with probabilities of legality and reliability of statements and claims of the parties as they could indicate more trust towards evidence that has passed certain standards to be analyzed by court.

One judicial problem is that banks cannot be expected to monitor and find every fraudulent transaction or unauthorized access before they happen, because that would be unreasonable and very expensive, and that is why customers are obliged by law to inform of unauthorized activity in the first place. At the same time use of electronic evidence on online services is evolving, so bank's responsibility to inform clients for safe use increases. In addition to severe financial losses, the clients may suffer from tension on social relations and trust issues between the service provider if they have been victim of fraud.[155] It is not clear how well these instructions are received by the clients.[156]

[155] Cassim, F. (2015). Potchefstroom Electronic Law Journal. – *Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thieves,* Vol 18, No: 2, p 75.

[156] Junger, M. (2016). Computers in Human Behavior. – *Priming and warnings are not effective to prevent social engineering attacks,* Vol. 66, p 77.

CONCLUSION

The aim of the research was to illustrate shift on burden of proof caused by controversial approach and interpretation of courts as well as negligence of parties in situation of court's lack of care while processing electronic evidence. Multinational case law and Finnish legislation were analyzed for better understanding of the topic to reader and to emphasize the existing problem. Thesis was structured to ascertain the general features and admissibility of electronic evidence, secondly to examine both appropriate and questionable case law to provide a comparative view for the scope of shift on burden of proof. Lastly, alternative options to enhance the knowledge of courts of electronic evidence, ensuring methods for maintaining qualification of courts and ascertaining the authenticity of electronic evidence were presented.

The lack of expertise and knowledge of courts tend to be the highest concern on scope of admissibility and authenticity of evidence, as was confirmed on case *Lorraine v. Markel American Insurance Company*. There is no doubt that some courts lack understanding of characteristics of electronic evidence. Occasionally they provide incomplete interpretation of law on expense of weaker proponent, provide more dignity for statements for party with higher authority, without challenging their correctness and adjust their own approach depending of the diversity of the matter. Such conduct and qualities ensure fundamental opportunities for burden of proof to be shifted, as was occurred on case *Bernt Petter Jørgensen v DnB NOR Bank ASA* and on *KKO: 2006:81*.

Frauds and unauthorized access on credit card or online banking accounts are excellent topics to examine the misinterpretation and lack of knowledge of courts, as they involve digital banking data as evidence, which must be examined with adequate means, regardless of the possible impact of status or authority of either of the parties. The expertise and capacity of court to dissociate false and unjustified electronic evidence play a significant role for court to ascertain the facts of the case. Relying for evidence of more influenced party without indicating appropriate analysis for counterclaims and evidence of other party alludes to disinterest and disregard of evidentiary obligations on court.

Shifting of burden or proof is considerably dependent on awareness and approach of the court to the electronic evidence as well as its capability to notice crucial and less valuable details and to separate them from the judgement.

The topic could be researched more by performing more wider investigation on both lower and higher courts and their actions on multiple countries while at the same time carrying more depth analysis to the challenges of admissibility of electronic evidence and its possible impact for traditional legal proceedings.

List of References

Scientific Books:

1. Barcelo III, J.J. (2009). *Burden of Proof, Prima Facie Case and Presumption in WTO Dispute Settlement*. USA: Cornell Law Faculty Publications.

2. Casey, E. (2011). *Digital Evidence and Computer Crime.*3rd ed. USA: Elsevier Inc.

3. Daniel, L.E., Daniel, L.E. (2011). *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*. USA: Elsevier.

4. Douglas, W. (2014). *Burden of Proof, Presumption and Argumentation.* USA: Cambridge University Press.

5. Hallberg, P. (2001). *Oikeudenmukainen oikeudenkäynti 2000-luvulla.* Finland: Talentum Media.

6. Hahto, V. (2008). *Tuottamus vahingonkorvausoikeudessa*. Finland: Talentum Media.

7. Hemmo, M. (2005). Vahingonkorvausoikeus. Porvoo: WSBookwell Oy.

8. Hock, L.H. (2008). *A Philosophy of Evidence Law: Justice in the Search for Truth*. New York: Oxford University Press Inc.

9. Lappalainen, J. (2001). *Siviiliprosessioikeus*. Finland: Talentum Media Oy.

10. Mason, S., Seng, D. (2017). *Electronic Evidence*. 4th ed. London: University of London.

11. Miller, C. (2012). *Evidence: Best Evidence Rule.* USA: CALI eLangdell Press

12. Niemi, J. (2010). *Civil Procedure in Finland.* Netherlands: Kluwer Law International BV

13. Tapanila, A. (2007). *Tuomarin esteellisyys.* Finland: Suomalainen Lakimiesyhdistys.

14. Virolainen, J., Martikainen, P. (2010). *Tuomion perusteleminen.* Finland: Alma Talent.

15. Wuolijoki, S. Hemmo, M. (2013). *Pankkioikeus.* Finland: Talentum Oyj.

Scientific Articles

1. Atkinson, J.S. (2014). Proof is not binary. - *Birkbeck Law Review*, Volume 2(2), 245-262

2. Bell, Graeme B. and Boddington, Richard (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?. - *Journal of Digital Forensics, Security and Law*: Vol. 5, No. 3 ,2-3.

3. Biasiotti, M.A. (2017). A proposed electronic evidence exchange across the European Union. – *Digital Evidence and Electronic Signature Law Review*, Volume 14, p 1-12.

4. Cassim, F. (2015). Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thieves. - *Potchefstroom Electronic Law Journal*, Vol 18, No: 2, p 68-98.

5. Goode, S. (2009). The Admissibility of Electronic Evidence. – *The Review Litigation*, Volume 29, Number 1, p 1-64.

6. Haybäck, G. (2009). Civil Law Liability for Unauthorized Withdrawals at ATMs in Germany. – *Digital Evidence and Electronic Signature Law Review*, Volume 6, p 57-66.

7. Heikkinen, P., Iivarinen, T. (2011). Ensuring trust in electronic payment media. – *Journal of Payments Strategy & Systems*, Volume 5, Number 2, p 162-169.

8. Hoffmann, A.O.I., Birnbirch, C. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. – *International journal of Bank Marketing*, Vol 30, Issue 5, p 390-407.

9. Junger, M. (2016). Priming and warnings are not effective to prevent social engineering attacks. - *Computers in Human Behavior*, Vol. 66, 75-87.

10. Kaplow, L. (2012). Burden of Proof. – *Yale Law Journal*, Volume 121, No 4, p 738-859.

11. Koivunen, T., Tuorila, H. (2015). Consumer trust relations with payment cards and banks: an exploratory study. – *International Journal of Consumer Studies*, 39(2), p 85-93.

12. Leroux, O. (2007). Legal Admissibility of Evidence. – *International Review of Law, Computers & Technology*, Volume 18, Issue 2, p 193-220.

13. Mason, S. (2012). Debit cards, ATMs and negligence of the bank and customer. – *Butterworths Journal of International Banking and Financial Law*, Volume 27, Number 3, p 163-173.

14. Mason, S. (2013). Electronic banking and how courts approach to evidence. - *Computer Law and Security Review*, No 29, p 144-151.

15. Mason, S., Bohm, N. (2017). Banking and fraud. – *Computer Law & Security Review*, Volume 33, Issue 2, p 237-241.

16. Nuth, M.S. (2012). Unauthorized Use of Bank Cards with or without the PIN: A Lost Case for the Customer?. – *Digital Evidence and Electronic Signature Law Review*, Volume 9, p 95-101.

17. Pavia, J. M., Veres-Ferrer, E. J. (2016). Is the cardholder an efficient alarm system to detect credit card incidents? – *International Journal of Consumer Studies*, Volume 40, Issue 2, p 229-234.

18. Plumer, G. (2017). Presumptions, Assumptions and Presuppositions of Ordinary Arguments. – *Argumentation*, Volume 31, Issue 3, p 469-484.

19. Porkess, R., Mason, S. (2012). Looking at debit and credit card fraud. – *Teaching Statistics*, Volume 34, Issue 3, p 87-91.

20. Pulina, M. (2011). Consumer behavior in the credit card market: a banking case study. – *International journal of Consumer Studies*, Volume 35, Issue 1, p 86-94.

21. Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. – *Identity in the Information Society*, Volume 3, Issue 1, p 175-194.

22. Räikkä, J. (2005). Global Justice and the Logic of the Burden of Proof. – *Metaphilosophy.* Volume 36, Issue 1-2, p 228-239.

23. Smedinghoff, T.J. (2012). Solving the legal challenges of trustworthy identity. – *Computer Law and Security Review*, Volume 28, Issue 5, p 532-541.

24. Thomson, L. L. (2013). Mobile Devices: New challenges for admissibility of electronic evidence. – *The SciTech Lawyer*, Volume 9, Number 3, p 1-5.

25. Van Der Meulen, N. (2013). You've been warned: Consumer liability in Internet banking fraud – *Computer Law & Security Review*, Volume 29, Issue 6, p 713-718.

26. Zipursky, B.C. (2015). Reasonableness in and out of negligence law. – *University of Pennsylvania Law Review*, Vol 163, No 7, p 2131-2170.

EU and international legislation

1. The Payment Services Act and Payment Institutions Act in addition to the EU Directive 2015/2366 on payment services in the internal market
2. Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Accessible: http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm, 16 April 2018.

Other countries' legislation

1. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 29.06.2016/533.
2. MaksulaitosLaki 297/2010, 30.04.2010.
3. MaksupalveluLaki 30.4.2010/290.
4. Oikeudenkäymiskaari 1.1.1734/4.

Court decisions

1. *Bernt Petter Jørgensen v DnB NOR Bank ASA*
2. BGH, Urteil vom 5. Oktober 2004 - *Az. XI ZR 210/03*

3. Kouvolan Hovioikeus, *KouHo:2012:3*, 5.1.2012.

4. Korkein Oikeus, *KKO:1994:82*, 8.9.1994.

5. Korkein Oikeus, *KKO:2006:81*, 16.10.2006.

6. *Lorraine v. Markel American Insurance Company*

7. *Pål-Gunnar Øiestad*

8. *United States vs. Albert Gonzalez.* United States Court of Appeals, First Circuit. NO. 00-1598. October 11, 2001.

9. *Z.S v Lietuvos taupomasis bankas*

Other Sources

1. Korttiturvallisuus. (2012) Shared Guidelines for Using Payment Cards. [Online] https://www.korttiturvallisuus.fi/en/Help/Reporting-misuse/ (March, 2012)

2. The Finnish Financial Ombudsman of Bureau (FINE). Ruling: PKL 75/11, point 1. Accessible: https://www.fine.fi/ratkaisutietokannat/ratkaisu/pkl-7511.html , 12 March 2018.

3. The Finnish Financial Ombudsman of Bureau (FINE). Ruling: PKL 77/11. Accessible: https://www.fine.fi/ratkaisutietokannat/ratkaisu/pkl-7711.html, 12 March 2018.

4. The Finnish Financial Ombudsman of Bureau (FINE). Ruling: PKL 4/12, points 30,33. Accessible: https://www.fine.fi/ratkaisutietokannat/ratkaisu/pkl-412.html 14 March 2018.