UiO : Faculty of Law
University of Oslo

Consumer liability in case of fraud with electronic payment instruments: an analysis of European and Russian rules

Candidate number: 8028

Submission deadline: 1 December 2015 (Autumn Semester, 2015)

Number of words: 16 972

Table of contents

Abbreviations

ATM	Automated teller machine
CNP	Card-not-presented (payment transactions; fraud)
CVV	Card verification value
ECB	European Central Bank
EEA	European Economic Area
EFTA	Electronic Funds Transfer Act
EMV	Technical standard for smart payment cards and for payment terminals, stands for Europay, MasterCard, and Visa
EU	European Union
ID	Identifier
IP-address	Internet Protocol address
NPS	National Payment System
PIN	Personal identification number
POS	Point-of-sale (terminals)
PSD	Directive 2007/64/EC on payment services in the internal market
PSD2	Proposal on payment services in the internal market 24.07.2013
SEPA	Single Euro Payments Area
SMS	Short Message Service
TILA	Truth in Lending Act
UK	United Kingdom
US	United States of America

1. Introduction

Since the electronic commerce offered to businesses a worldwide market via the Internet, traditional paper payments such as cheques or cash seem likely to be replaced by electronic payments. The convenience of payments with credit cards, digital cash or via online banking made them popular between all users all over the world. In spite of the possible negative consequences, the use of electronic payments today is the key means to successful activity of the merchants, satisfaction of consumer's needs and prosperity of the economy in whole.

However, the efficiency of the electronic payment instruments does not exclude their substantial failure. Otherwise speaking, this type of payments is highly susceptible to fraudulent activity. Electronic payment fraud with its multi-billion dollar damages creates deadweight loss for the entire economy by increasing the cost of payments for the participants of the payment transaction and by the draining of the private banking accounts.[1]

In most cases it is extremely difficult to identify the person who has committed fraud and to recover stolen funds. Therefore, the allocation of losses has become the challenging issue. Economically, such losses are calculated and laid in the price of goods or services by the merchants, issuer banks and the card network corporations. Relative to consumers, these participants have ability to spread these losses and they possess superior information about their risks. Consumer has no ability to predict these risks and losses. That is why he needs to be protected by law as the weaker party in electronic payment relations.

However, the loss allocation rules are important not only because of their distributional consequences between interested parties. Good legislation can also promote economic development by reducing the costs for the cash circulation and by making the payment system more transparent. To achieve these goals the law should create comfortable environment for the consumers who can trust to the payment networks and the financial institutions.

Moreover, proper rules can create right incentives between the parties. It means that the stronger party would feel the greater liability for the losses. Practically, this will force the banks and card network corporations to develop better security measures to avoid fraud. Consumers, in their turn, would feel the liability for the payment instruments and be cautious to the order of their use. The methods used by scammers are constantly evolving and the law is often behind the technology. The right incentives could make a law progressive and the rules workable despite technological changes.

[1] Levitin, "Private disordering? Payment card fraud liability rules", 2

In the light of this issue, two legal frameworks - the European Payment Service Directive and the Russian Law on the National Payment System will be examined in this paper. Additionally, the US liability regime needs to be presented: this alternative approach significantly differs from the above mentioned legislations and it creates completely other environment for the participants of the electronic payments.

The paper's discussion will revolve around the following basic questions:

- Does the loss allocation regime established by these laws properly determines the liable party in the case of the fraudulent payment transactions?
- Does the consumer have enough rights and possibilities to reimburse his losses if he did not act fraudulently?
- Do these laws induce financial institutions to take the optimal level of protection for consumers to avoid unauthorized withdrawals?
- What kind legal improvements should be done today to support the consumer as the weaker party of the electronic payment transfer?

All these questions will be analyzed in this paper.

1.1 Methodology

This paper focuses on the issue of loss allocation caused by unauthorised electronic payment transactions initiated without consent of the payer. Generally, such transactions are executed by fraudsters. Thus, the questions “who is liable” and “who will bear the losses” in this situation arise between the participants of the electronic payment transfer: consumer, merchant, issuer bank, acquirer bank and card payment association. This paper is dedicated primarily to analysis of the consumer liability as the most vulnerable party in these relations. The issue will be observed on the basis of two legal frameworks of the European Union and the Russian Federation: recent revision of the payment legislation by the European Commission, lack of detailed analysis of the gaps in the current Russian law and limited literature regarding this problem in the context of these two neighbor regions prompted me to choose this subject.

First, I will present the relevance of the issue by introducing diversity of the types of fraud and the statistical data of the fraudulent transactions. Secondly, I will discuss the current liability regimes established by the European and Russian legislators. Further, the examples of the case law will be analyzed to stress the weaknesses of the recent regulation in dealing with the problem of fraudulent use of electronical payment instruments on the consumer level.

In the fourth chapter I will discuss the advantages of the alternative US zero liability policy and assess the role of other participants of electronic payment transactions. Finally, the new legislative proposals within the European Union and additional measures against fraudsters will be examined with regard to conclusions that have been formulated in the previous chapters. The opinions and criticism which have been formulated by European, Russian and American scholars also will be employed in this paper.

1.2 Types of fraud with electronic payment instruments

One of the most important transformations of the Internet in the last decade of its existence is that the Internet has become a tool for satisfaction of our daily needs, for example, we use it to do online shopping and to check bank statements. Thus, the importance of electronic payment instruments has considerably increased, as has the number of cybercrimes.

It is beyond the scope of this paper to go into a detailed discussion of all areas of cybercrimes; rather the focus of discussion in this paper is fraud with electronic payment instruments, such as credit and debit cards, credit transfers and direct debits.

Generally, a payment instrument means "any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order."[2] The electronic character of the payment instrument specifies that transfers should be non-cash and executed via the remote access (or by using personalised devices).

In contrast to traditional paper methods of payments, the lack of face-to-face interaction with the fraudster, which allows for more anonymity, makes the electronic payments so susceptible to crime. The evolution of methods used by perpetrators additionally promotes the growth of online crimes and online card fraud in particular.[3] In any case payer or issuer of the payment instrument bears the losses and the type of fraud can be decisive in the question of liability.

Bhattacharyya and others divide card fraud for two types: application and behavioral fraud[4]. In application fraud criminals obtaining new cards from issuing companies using false information or other people's information.

---

[2] European Commission, Directive 2007/64/EC of the European Parliament and 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, OJ.L. 319, article 4.23

[3] van der Meulen, “Between awareness and ability”, 14

[4] Bhattacharyya *et al*., “Data mining for credit card fraud”, 603

Behavioral fraud can be performed in a number of ways:

- Non-receipt fraud occurs when perpetrators tap credit cards in transit before they reach cardholders or steal personal information from bank and credit card statements;
- Stolen/lost card fraud happens when fraudsters capture credit cards through theft of wallet or gain unauthorized access to lost cards;
- Counterfeit card and "card-not-present" (CNP) fraud utilizes credit card-sized plastic with account numbers and names embossed on the cards without the knowledge of card holders for to conduct CNP transactions, i.e. through mail, phone, or the Internet;

Obtaining of the card holders information may occur in the following ways:

- Skimming involves stealing credit card information during a legitimate transaction. This scheme usually occurs in businesses where the credit card is taken out of sight while the transaction is processed. The fraudster will swipe the card through skimming device (the "wedge"), which records all information contained on the magnetic strip. Information then can be used for selling and producing counterfeit cards;
- Phishing occurs when criminals create websites that appear to be from trusted organizations (for example, banks, eBay, PayPal) where cardholders enter in personal information such as username and credit card details. The fraudsters send out a large amount of emails (the "bait") directing the victims to their phony web sites. These sites are easy to set up and even if a small number of victims fall for the scheme, the fraudster can profit by stealing the victim's identities and then stealing their money[5];
- Stealing information by employees of the banks, restaurants, etc.
- Intrusion into company computer networks, hacking banking system or online auctions, cyber-attacks and malware campaigns.

For the purposes of detection card fraud can be distinguished for online and offline fraud.[6] Offline fraud is committed by using a stolen physical card at a storefront or call center. If the theft is discovered quickly enough, the issuer institution can lock instrument before its unauthorized use. In online fraud which occurred via web, phone shopping or CNP manipulation fraudsters use only card's details; a manual signature and card imprint are not required for online purchases.

One key distinction considers how hackers can steal data. The two most common ways are manually, where the perpetrators retrieve data during the time that they are infiltrating a

[5] Barker *et al*., "Credit card fraud", 403

[6] Wei *et al.*, "Effective detection of sophisticated online banking fraud", 455

computer, and through a concealed automated program, such as virus or malware installed in the victim's computer.[7] The latter method is more dangerous because malware lies in wait to copy and transmit data as it become available. Even if the user does not store information malware can capture it. Once hackers obtain the information, they can easily produce a counterfeit card for to pay in stores (card-present transactions) or may use data to shop over the internet or phone (CNP transactions).

One of the latest forms of the credit card fraud today is chargeback or so-called "friendly" fraud. It occurs when a consumer buy items online, receive and keep them, but then dispute the charges on their bills, saying they never made the purchases or the merchandise never arrived. The credit card issuer withdraws the money for the transaction from the merchant's account and returns it to the customer. As a result, the merchant loses the merchandise and money for the transaction and in some cases pays a chargeback fee.

Fraudulent Internet banking activities are developing on a par with the widespread use of Internet technology and e-commerce. Undoubtedly, it bears negative consequences and raise quite complex and serious issues for all participants: financial institutions, merchants and consumers. To assess the importance of the problem the next chapter will be looking at an alarming statistics relating to the card fraud within the European Union and Russian Federation.

1.3 Fraudulent payment transactions statistics

Every year credit cards of thousands of consumers are used fraudulently, and there are over 100 different sources of data on cybercrime which provide with numerous surveys about cybercrimes. However, many of these surveys have a particular view and specific agenda. Moreover, such kind of statistics can be insufficient and fragmented because of possible under- and over reporting and dependence on who collected them. Errors which appear also may be intentional (e.g., vendors and security agencies playing up threats) or unintentional (e.g., response effects or sampling bias).

The more prominent sources include surveys from national authorities and police agencies (e.g., Eurostat, CSI and consultancies); security breach disclosure reports; direct observations of attack trends from antivirus software vendors (e.g., from Symantec, McAfee and

[7] Segal *et al.*, "Credit card fraud: a new perspective on tackling an intransigent problem", 757

Microsoft); and reports by trade bodies (from banking trade associations, or the Anti-Phishing Working Group).[8]

The starting point for the aim of this chapter will be the Fourth report on card fraud issued by the European Central Bank (ECB)[9] in 2015 and the Survey about unauthorized money transactions 2014 released by the Central Bank of the Russian Federation (Bank of Russia).[10]

In January 2008 the ECB's Governing Council approved an oversight framework for card network associations. As a result, each association is asked to supply general business data and state the number and value of fraudulent and total transactions for each EU Member State, as well as for the Member States of the European Free Trade Association (Switzerland, Iceland, Liechtenstein and Norway which are also SEPA)[11].

This report summarizes the information for the year 2013 received from the 23 card network associations, such as MasterCard Europe, Visa Europe, American Express, BNP Paribas Personal Finance, etc. Payments made with cards issued outside SEPA and acquired within SEPA have been included in this report also.

Chart 1 represent the total value of card fraud using cards issued within SEPA and acquired worldwide amounted to €1.44 billion in 2013, which represented an increase of 8.1% from 2012. In relative terms, i.e. as a share of the total value of transactions, fraud rose by only 0.001 percentage point, i.e. from 0.038% to 0.039% in 2013. However, in spite of this rise the share of the total value of fraudulent transaction in 2013 is lower for 0.009% percentage point than in 2009.

From the types of card fraud perspective, 66% of the value of fraud resulted from CNP payments, i.e. payments via the internet, post or telephone, 20% from transactions at point-of-sale (POS) terminals and 14% from transactions at automated teller machines (ATMs).

With €958 million in fraud losses in 2013, CNP fraud was not only the largest category of fraud in absolute value but, unlike ATM and POS fraud, also the only one recording an increase compared with the previous year, with growth of 20.6% from 2012.

The largest drop in the level of fraud was experienced by card fraud committed at ATMs, with 13.7% less fraud in 2013 than in 2012, the first time in four years that ATM fraud fell. Fraud committed at POS terminals went down by 7.9%. The reasons of that were mainly a

[8] Anderson *et al.*, "Measuring the Cost of Cybercrime", 267

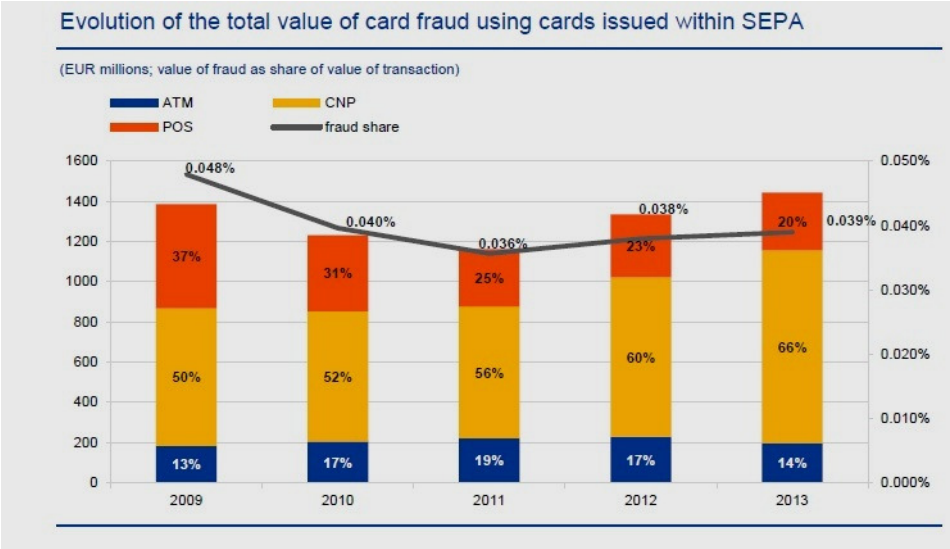
[9] See online at: https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

[10] See online at: http://www.cbr.ru/psystem/P-sys/survey_2014.pdf

[11] Mentioned Member States constitute the Single Euro Payments Area (SEPA) which was created by the EU for the simplification of bank transfers and for making all electronic payments in the euro area as easy as cash payments and under the same basic conditions, rights and obligations, regardless of their location.

result of a decrease in counterfeit fraud levels and, from a geographical point of view, due to decreases in cross-border fraudulent transactions acquired within SEPA (€566 million losses on non-SEPA-issued cards used inside SEPA against €320 million losses on SEPA-issued cards used outside SEPA).

Chart 1. Evolution of the total value of card fraud using cards issued within SEPA[12]



The collected data on the Survey from the Bank of Russia was based on the Russian private banks reports. It was the first time when the Bank of Russia released such kind of survey, and, somehow, it refers to the statistic from the Second and the Third reports on card fraud of the ECB.

Unfortunately, there is no data to compare figures for the previous years, but nevertheless, it would be meaningful to observe the volume of the fraud within the Russian Federation in 2014.

In the year 2014 the total value of cards fraud amounted to €77.83 million losses, while only €35.13 million was committed with the cards issued by the Russian banks. It should be noted also that fraudulent transactions accounted for 0.057% from total volume of card transactions. With the share of 65.8% CNP fraud was the largest category in the total fraud, but the volume of the losses actually was equal with the volume caused by ATM and POS fraud – 38.5% and 37.5% relatively. Comparative percentage of total cards fraud in terms of value is represented in chart 2.

[12] European Central Bank, the Fourth report on card fraud of 15 July 2015, 7

Chart 2. Percentage of total card fraud in terms of value[13]

Percentage of total card fraud in terms of value	Europe	USA	Russia	Australia	Canada
Year	2013	2012	2014	2013	2013
Card not presented	66	40	72	72	61
Card presented (ATM+POS)	34	60	18	28	39
Counterfeit/skimming	15			12	29
Lost/stolen	15		10	11	5
Card not received	1	Not available		3	1
Fraudulent application				1	2
Other	3			1	2

The positive trend towards to the drop in ATM and POS fraud presented both in Europe and Russia could be supported by the migration to the EMV standard (smart cards with chip).

Both reports indicate noticeable increasing trend in CNP fraudulent transactions, which is expected to grow further. Only during 2014 the number of CNP fraud in Russia increased by 44.8%, but it is obvious, that the volume of losses within the Russian Federation is not comparable with the European.

However, according to information collected by the leading Russian company Group-IB which specializes in preventing and investigating cybercrimes, the real total value of losses in Russia counts €2.22 billion. *This amount is not only substantially bigger than the figure from official survey of the Bank of Russia, but even considerably exceeds losses within SEPA*[14]. Furthermore, we can observe that the number of authors also referred to the same issue, i.e. the lack of transparency in the assessments of financial damages, in Europe and all over the world (Bolton R., 2002, p. 238; van der Meulen N., 2013, p. 713; Schudelaro Ir. A.A.P., 2001, p.107).

Group-IB identifies several reasons of this discrepancy. First of all, Russian banks avoid to disclosure information about their clients. Secondly, they do not include in statistical data cases when stolen money was returned to their clients. Finally, when the clients laundered funds and lays these remittances as hacker attacks, banks try not to attract the attention of the regulator because of the possible liability in the client's crime.

In conclusion, based on the statistics above, one can say that the card fraud is a very attractive and highly profitable type of financial crimes today, which is hard to account, prevent and investigate. That is why legal issues and regulation of electronic payment transactions have become inevitable for society.

[13] European Central Bank, the Fourth report on card fraud of 15 July 2015, 11; Bank of Russia, the Survey about unauthorized money transactions 2014 of July 2015, 6

[14] Aleshkina, "The Bank of Russia disclosed the volume of fraudulent transactions"

2. Regulation environment of the electronic payments in the EU and Russian Federation

The statistical data from previous chapter indicates the relevance of the electronic payment fraud. Notably that in most of the cases it is hard to find the offender. Consequently, one of the parties of the electronic payment (payer, payee, bank) has to take the liability for the fraudster's enrichment. Because of the obvious reluctance of the participants to bear such losses, legislators imposed legal rules for to determine the liable party. In the second chapter I will consider the liability regimes established by the European and Russian law which intended to regulate loss allocation issue.

2.1 The liability regime under the EU Payment Services Directive

2.1.1 Background and perspectives of payment services regulation in Europe

Regulation of electronic payments in Europe begins from the SEPA implementation, where single market of electronic payments for consumers and businesses across the euro area should have the same level of efficiency and security as in their home countries. Since the integration of this initiative, the "modernization and consolidation of the Eurozone payments infrastructure and the development of cross-border payment products"[15] have come to the fore. However, the diversity of the national legislation created difficulties for realization of these aims and discouraged the growth of e-commerce within the SEPA.[16]

For to harmonize various national rules the Commission issued a non-binding Recommendation[17] that applied to all transactions involving instruments that allow remote access to the holder's account, such as transfers of funds and cash withdrawals effected by means of an electronic payment instrument and the loading and unloading of an electronic money instrument. It prescribed minimum information requirements and the obligations of the issuer and holder and provided for the protection of payment cards customers.

The transposition of the Recommendation's provisions into national legislation has been recognized as insufficient.[18] In fact, only Belgium formally transmitted it into national law

[15] Janczuk, "The single payments area in Europe", 322

[16] Mercado-Kierkrgaard, "Harmonising the regulatory regime for cross-border payment services", 177

[17] European Commission, Recommendation 97/489/EC of 30 July 1997 concerning transactions carried out by electronic payment instrument and In particular the relationship between issuer and holder, OJ.L. 208, 02.08.1997, 52

[18] European Commission, "Communication from the Commission to the Council and the European Parliament concerning a New Legal Framework for Payments in the Internal Market", 9

system. Moreover, the additional legal provisions from the several European directives on taking up and pursuit of the business of credit institutions were fragmented, overlapping and in some cases contradictory for regulation of electronic payments.[19]

In order to boost consumer confidence and to foster trade, by the end of 2007 the Commission proposed the European Directive on payment services (PSD). [20] In contrast to Recommendation, the PSD had to be incorporated by all Member States and it has changed situation dramatically. More specific, the PSD gave to the holders of electronic payment instruments higher level of protection and improved legal clarity by standardization of rules. Moreover, the Direction has become a significant attempt to achieve a balance between consumer protection and payments market liberalization and, as a result, the value of payment transactions in the EU increased from €594.5 billion in 2010 to €240.24 trillion in 2012[21], what explicitly underlines the positive impact of this legislation.

Nevertheless, technology and business models inevitably lead to the need for revision of the acting rules. Therefore, it is important to note that from July 2013 the EU Commission has already begun to revise the current legislation for to ensure more secure and convenient electronic payments in Europe and to support a new generation of payment companies.[22]

2.1.2 Unauthorised payment transactions and the liability of the payment service provider

According to Levi, "the global networks, credit, debit and charge cards can never avoid the risk of crime entirely".[23] Taking into account this statement, one of the participants of the electronic payment anyway has to accept responsibility and losses.

In contrast to the Recommendation, the PSD allocates the liability when a payment transaction is unauthorised. Article 54.1 of the Directive sates, that "a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction". Hence, in the absence of such consent transaction shall be held unauthorised.

The procedure for transmitting consent must be agreed between the payer and the payment service provider (article 54.4). Moreover, consistently article 42.2 it is necessary to incorporate the form of and procedure for giving consent in the contractual conditions which

[19] Mercado-Kierkrgaard, "Harmonising the regulatory regime for cross-border payment services", 179

[20] European Commission, Directive 2007/64/EC of the European Parliament and 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, OJ.L. 319

[21] London Economics and iff in association with PaySys, "Study on the impact of Directive 2007/64/EC", 271

[22] See online at: http://ec.europa.eu/finance/payments/framework/index_en.htm

[23] Levi, "New Frontiers of Criminal Liability", 229

must be communicated in good time before the payment service user (i.e. client or payer) is bound by any contract. The conditions also must be set out in easily understandable words and in a clear and readable form, take place on a paper or on a durable medium in a manner accessible for future reference (article 41.1).

The distinction between transactions taking place before notification of loss, theft or misappropriation of the payment instrument and transactions taking place after notification also has become crucial provision for dividing liability in the case when transaction is unauthorised.[24] As a result, the Directive in the articles 56 and 57 imposes significant obligations relating to the notification on the payment service provider (i.e. bank which issued electronic payment instrument) and the payment service user.

In the light of this point, the payment service provider bears the financial consequences which occur after notification about lost, stolen or misappropriated payment instrument. Article 61.4 excludes the liability of the payment service user as soon as notification has taken place and he has not acted fraudulently. Whether the payment service provider is actually able to prevent further use of the instrument is irrelevant in this case.

Moreover, according to article 57 of the PSD the payment service provider must ensure that appropriate means are available at all times, enabling the payment service user to notify the loss, theft or misappropriation of payment instruments. Therefore, it must be possible to notify loss or theft seven days a week on a twenty-four hour basis.[25]

When the payment service provider does not fulfill the obligation of providing appropriate means, the specific sanction will apply, i.e. the provider will be held liable for all transactions which have taken place before the user tried to notify him and until actual notification.

From the other side, the payment service user bears the losses deriving from the use of a lost or stolen payment instrument or, if the user has failed to keep the personalized security features safe from misappropriation of a payment instrument, occurring before he has fulfilled his obligation to notify the provider. The limit of such liability restraint to €150, unless the user has acted fraudulently or has failed to meet the obligations imposed on him by article 56 with the intent or gross negligence. Thus, if the user acted fraudulently or with gross negligence article 61.2 lays full liability on him.

[24] Steennot, "Allocation of liability", 556

[25] Ibid, 556

2.1.3 Gross negligence and liability of the payment service user

Whether the payer has acted negligently is the challenging issue in the question of liability and bearing the losses. The concept of gross negligence is not determined in the PSD, and what exactly entails gross negligence is quite ambiguous. Article 61.2 of the Directive only designates that the payer is liable without limitation in case of gross negligence with regard to his obligation under the article 56.

Pursuant to the article 56, the payer has to: a) use the payment instrument in accordance with the terms governing the issuing and use of the instrument; b) to notify the payment service provider, or the entity specified by the latter, without undue delay of loss, theft or misappropriation of the payment instrument or its unauthorised use and c) to take all reasonable steps to keep safe the security features of the payment instrument.

Unlike the article 6.1 of the Recommendation, the PSD does not state that the payer is liable without limitations as soon as he violates one of these obligations. Only if the court decides that the certain behavior or violation constitutes gross negligence, it will lead to unlimited liability of the consumer. The lack of the gross negligence definition leads to the situation where "the terms "careless" and "negligent" differ per case, per client and per bank."[26] For example, the Court of Appeal in Belgium decided that gross negligence requires something more than mere carelessness.[27]

The obligation in the article 56.2 of the Directive alters unnecessary concreteness of the article 5 (c) of the Recommendation, where it was prohibited to record the personal identification number (PIN) on the instrument in an easily recognizable form. Situation becomes controversial when the PIN can be recorded on the instrument but in an encrypted form.

For example, in Germany the Court of Kassel decided that a card holder that incorporates his PIN in a phone number, written down on a paper in his wallet, acted negligently.[28] In the UK HSBC refused to refund stolen money to a couple which wrote their PIN in a heavily disguised form on a business card held in purse. Bank also stated that there were no incorrect PIN inputs, no balance inquiry, and no further attempted withdrawals after the cards were reported stolen.[29]

---

[26] van der Meulen, "You've been warned", 714
[27] Steennot, "Allocation of liability", 557
[28] AG Kassel 16.11.1993, W.M. 1994, 2110
[29] Brignall, "Now banks are trying to pin the blame for card fraud on you"

In the Netherlands, it was determined that a card holder did not act extremely negligently, when he incorporated his PIN in a phone number, written down in his agenda with several phone numbers.[30] Therefore, the outcome depends on the circumstances of the case, and the lack of clarity gives the judge a right to decide at his discretion.

According to study on the implementation of Recommendation 97/489/EC[31], the late notification also constitutes gross negligence. It means that if the payment service user finds out that his card is stolen, lost or misappropriated, he must act without delay. When it is impossible to prove the actual knowledge of loss or theft of the instrument, the payment service user should have been aware of loss or theft.

Following the last statement, the question arises whether a card holder has to control continuously location of the instrument. At least in Belgium, this is not the case.[32] For instance, the Court of Appeal in Brussels decided that a card holder does not act grossly negligent if he only discovers missing of the card after one month.[33] In another case, the same Court argued that in case when person gets its wallet back, that has fallen out of pocket, he does not need to verify immediately that the presence of card after return.[34]

It should be noticed that in the case of late notification the holder will be liable for all transactions that have taken place before notification. The fact that the holder has become aware does not change the limits of liability for him. As it was stressed before, late notification must be regarded as a gross negligence. Hence, the possibility to reduce the holder's liability in the case of late notification from the moment when the holder has been aware is excluded.

At the conclusion a final remark must be made. The current Directive has prescribed common rules for all Member States, which allocate the liability between issuers and users of electronical payment instruments. In contrast to the Recommendation, it was a great step forward for harmonizing legal framework within SEPA. Unfortunately, the Directive also has several drawbacks, such as lack of clarity and consistency, which made the consumer dependent on the circumstances of the fraudulent case and the decision of the court. These weaknesses will be discussed in greater detail in the third chapter.

---

[30] GCB 24.09.1994, T.V.C. 1995, 183
[31] CRID, Study on the implementation of Recommendation 97/489/EC, 76
[32] Steennot, "Allocation of liability", 557
[33] Brussel 27.05.2002, NjW 2003, 311, T.B.H. 2004, 158
[34] Brussels 04.10.2005, Bank Fin.R. 2006, 148

2.2 The liability regime under the Russian law on the National Payment System

2.2.1 The implementation of new legal framework

According to the Russian statistics, the proportion of cash circulation in Russia is still higher than in other foreign countries.[35] Undoubtedly, its reduction can significantly cut budget costs, escape non-transparency of the payment system and create additional incentives for economic development. However, the regulation of the electronic payments in Russia inevitably lags behind the existing realities.

Before the implementation of the Federal law "On the National Payment System" (NPS law)[36] in 2011, the Russian payment transactions was governed by the Civil Code of the Russian Federation as well as by various federal laws[37], in particular those applying to the Central Bank of the Russian Federation; banks and banking activity; and the postal service.

This previous legal framework had a huge drawback, i.e. there were no special rules for regulation of electronic payments. Furthermore, these uncodified laws did not consider the technological development of payment instruments that happened over the past decade. As a consequence, the lack of the single approach and key definitions created a negative effect on the Russian economy as a whole, and law enforcement and consumer protection, in particular.

Since the early 1990s, there have been several attempts to build a national payment and clearing network but no concrete action ever followed the proposals. Situation has radically changed with the adoption of mentioned NPS Law, which has become the most serious step towards regulation of payments.

At the beginning, the proposed law pursued the realization of the following objectives: promotion of credit cards use among citizens; development of electronic payment infrastructure and improvement of its efficiency; harmonization of banking standards for interaction with international settlement systems[38]. However, with the imposing sanctions and changes in the political situation these objectives partly lost their relevance.[39] The greater protection of the privacy of Russian card holders and reducing dependence on western payment institutions has moved the primary focus to setting up a national payment network which would allow processing all electronic payments inside the country.

---

[35] Korotaeva, "Problems and development prospects of non-cash retail payments in Russia", 170

[36] State Duma, Federal Law "On the National Payment System" N 161-FZ of 27 June 2011, RG N 5515, 30.06.2011

[37] Federal law means that it operates in all federal subjects of Russia

[38] Obaeva, "National payment system", 34

[39] See online at: http://ftalphaville.ft.com/2014/04/25/1837182/guest-post-making-a-non-western-payment-card-system-in-russia/

Nevertheless, regardless the political background, the new NPS law establishes following important provisions concerning consumer protection and electronic payments:

- Introduction of a number of key definitions, such as payment services, electronic payment services, payment system, electronic payment instrument and electronic money;
- Providing the payment service providers and their customers with the necessary set of rights and obligations for the use of electronic payment instruments;
- Regulation "of the various types of operators offering money transfer services (including those involved in the booming business of international remittances)"[40];
- Providing a legal framework for mobile network operators offering financial services on the mobile phone and specialized e-money operators;
- Expanding the functions of the Central Bank of the Russian Federation in terms of registration and maintenance of the registry operators of payment systems to ensure the stability of payment transfers.

Entry into force of the NPS law was gradual. The article 9 which is dedicated to the use of electronical payment instruments became effective only on 1st January 2014. The reason of it was largely in unavailability of financial institutions to operate under the new rules. However, a huge increase of fraudulent card transactions has become an additional incentive for its faster implementation. The next subsection introduces the new legislation concerning to electronic payment transactions in more detail.

2.2.2 Regulation of electronic payment transaction under the NPS law

As it was mentioned above, the new regulation of electronic payment transactions came into force only from the beginning of 2014. According to the Bank of Russia, in July 2013 only half of all Russian banks were ready to fulfill the requirements of the new law[41]. However, despite numerous criticisms, it was inadvisable to postpone its implementation.

Article 9 of the NPS law determines the procedure for the use of electronic payment instruments. The starting point of this article defines the basis for legal relationships, which occur between the payment service operator (i.e. bank, service payment provider) and the client (i.e. payer, payment service user) in use of electronic payment instruments.

[40] Staschen, "Financial Inclusion and Innovation in Russian Payment Systems"
[41] Gorovcova, "Refund for unauthorized transactions", 3

This relationship is based on the form of a contract, which according to article 401 of the Russian Civil Code[42] is considered as a guarantee of proper fulfillment of obligations and possibility to obtain compensation for damages in case of violation of the undertaken obligations by the parties. Notably that from the one side, the reference to the Civil Code gives additional safeguards for electronic payment transactions. From the other side, this legal approach allows the operator to give a direct refusal to the client in concluding the contract, what makes the position of the client initially weaker (article 9.2 of the NPS law).

Moreover, the NPS law says nothing about essential conditions and the form of such contract. The legislator did not include these provisions in the law, relying apparently on the chapter 28 "The Conclusion of the Contract" of the Russian Civil Code. However, the NPS law states in the article 9.3 that the client must be informed before signing of the contract about the conditions of use of electronic payment instruments, in particular any limitations and possible high-risk character of their use. The operator is also obliged to give documents and information about the use of payment instrument after conclusion of the contract (article 9.7).

Generally, to a certain extent the excessive regulation may hinder proper development of electronic payment services, but from the standpoint of consumer protection such a situation is undesirable. It is undeniable to my mind that explicit contract terms about payment service operator, charges, interest, exchange rates, the means of communication, including the technical requirements, etc. would help to avoid potential disputes between the parties in the future.

2.2.3 Allocation of liability between operators and customers

The key point to determine which party will be liable for damages, when an electronic instrument is stolen or used without the consent of the owner, depends on notification. According to article 9.4 of the NPS law, the operator is obliged to inform the client about every electronic payment transaction by sending him a notification. The procedure of sending notification should be described in the contract. At the same time, the client has to provide the operator accurate contact information and in case of changes he has to notify operator in a timely manner (article 5.13). The operator, in its turn, is considered to have fulfilled its obligation to notify when it has sent a notification to the client.

[42] State Duma, the Civil Code of the Russian Federation, N 51-FZ of 30 November 1994, RG N238-239, 08.12.1994

However, the NPS law states nothing about the receipt of the notification by the client, the manner of such notice, nor the period during which that obligation has to be executed. One must suppose that these omissions can be rectified via the contractual provisions[43], but this lack of clarity in the legal framework carries a great risk for the operators and their customers. According to article 9.13, if the operator has not fulfilled the obligation to inform the client about a payment transaction, he shall reimburse the amount of payment to the client, if it was made without the latter's consent.

The operator does not bear liability, if the customer received the notification from the operator, but did notify the latter in an agreed form without undue delay that the payment instrument was stolen or used without consent. It should be noted, that the customer has only *twenty-four hours* to inform the operator for avoiding liability and damages in the case of unauthorized transaction.

Article 9.15 establishes a similar procedure for liability in the case when the client is an individual. Indeed, the operator has to bear all loses if individual has sent the notification in a right time and the payment transaction was executed without consent, which implies unlimited liability of the operator. However, the operator has the right to prove that the customer has violated the order of the use of electronic payment instrument. If the violation is proved, the liability will born by the individual.

Following this point, it may seem that the legislator has totally protected the interests of consumers, putting the operators in a weaker position. On the other hand, the law states nothing about partial liability of the customers (e.g. loss limit maximum within €150) and fraudulence with electronic payment instruments. It is obvious, that bank will try to prove that client used the payment instruments in violation of the applied order. Eventually, the decision will be taken in the court as the final authority, what makes consumers highly dependent on the circumstances of the case.

2.3 Findings of the Second Chapter

In conclusion of this chapter, one can state that legislators in Europe and Russia have established different methods to allocate the liability between the issuers and users of the electronic payment instruments. From the one side, it may seem that the Russian consumer is more protected than the European, because the Russian consumer can be only held liable under two simple and comprehensive conditions: he has to obtain a notification from the

[43] Chirkov, "Problems of realization of legislation on national payment system", 65

operator about the payment transaction and he in his turn has not sent notification to the operator about the lost, stolen or misappropriated payment instrument. However, the legal failures such as the form of notification receipt, the absence of explicit contractual conditions between the client and the bank, the limit timeframe for notification of the operator eliminate the previous advantages. It is obvious, that such lack of clear rules will have a negative impact on consumer protection and law enforcement as a whole.

3. Law enforcement: issues and consequences

In the previous chapter we considered the European and Russian legal frameworks which constitute the loss allocation rules in the case of unauthorised electronic payment transactions. Both the European Directive and the Russian NPS law have several drawbacks which facilitate the rise of court litigations between the issuers and the users of the payment instruments. The next chapter introduces examples of the case law where the loss allocation issue and its regulation will be analyzed from a practical perspective.

3.1 The problems of law enforcement within the European Economic Area

3.1.1 Examples of negligent behavior in different jurisdictions

In general, the common conception within European Union states that banks reimburse the financial losses of their clients as victims of fraud with electronic payment instruments.[44] As it was mentioned in the subsection 2.1.3, the payment service user, however, bears all losses resulting from the fraudulent use or default of obligations of use of electronic payment instrument with intent or gross negligence.

Nevertheless, determining the liability of participants in the case of gross negligence is a challenging issue. More specifically, there is no explicit interpretation about the qualification of gross negligence. Since the term is open to explanation, decisions made by different banks can even be conflicting despite a similar set of circumstances.[45]

Van der Meulen gives an example of two cases which occurred in different banks in the Netherlands, but with resembling facts. Two individuals, who are customers of the ABN Amro bank and Rabobank, received a same phishing email. After having read messages, customers got phone calls from persons who claimed to be banking employees. The fraudsters

[44] van der Meulen, "You've been warned", 714
[45] Ibid, 714

enounced that the clients had to be checked and verified for potential errors. Thus, fraudsters obtained the data from random reader codes of clients and drained their accounts.

The subsequent decisions made by the banks demonstrate the potential arbitrariness.[46] The client of the ABN Amro was refunded, whereas the Rabobank declined to reimburse losses. The Rabobank regards that client acted negligently when he provided the codes to another person. In order to enhance its position, Rabobank states that ignoring their warnings about this type of attack which were specifically posted on the Internet banking screen, also proved negligent behavior. Hence, such *consumer awareness* was considered as enough reason to shift liability from the bank to consumer.[47]

This tendency was also supported by the German Federal Court of Justice which ruled that the man was negligent when he remitted money using 10 transaction numbers, also known as TAN codes. The codes are commonly used for verification of accuracy of given online transactions in Germany. However, the man entered his TAN codes onto a website designed to look like his bank's site, Sparda Bank.[48] The court stated that the bank was not liable, as it had specifically provided warnings to its customers against this type of fraud.

Following these examples from the Netherlands and Germany, one point can be distinguished to determine whether the client acts negligently. If client was warned about "known" attack, than bank will likely refuse to refund losses considering this as a negligent behavior.

Unlike above mentioned outcomes from the consumer awareness, the Financial Ombudsman Service in the UK decided a similar scam case in favor of the client (case study 116/09). Mrs. J received a phone call from her bank to tell that her card had been cloned and that she should ring another department at the bank immediately.[49] Mrs. J rang the number from her debit card, answered on the security questions and told the log-in and PIN details. After three days she realized that she had been the victim of a scam fraud and asked her bank for reimbursement. The bank insisted that it was a case of gross negligence, where the client gave her security details to the fraudsters and ignored warnings on never giving out full passwords, even to the bank employees, on their online banking site. However, the financial ombudsman stressed that *the client herself had not authorised the transactions* and told the bank to refund all money to the client.

[46] Ibid, 714
[47] Ibid, 715
[48] Farivar, "Clients, not banks, liable for losses in phishing scams, court rules"
[49] Financial Ombudsman Service in the UK, Disputed transactions case studies, 13

Another example to determine the aspects of gross negligence can be presented from the Norwegian case law. According to Nuth, the wrong tendency of Norwegians courts to lean towards banks was demonstrated in the Øiestad case.[50] A credit card from Master card was stolen and debited with over NOK 50 000 before it was cancelled. The bank argued before the Complaints Board and the District Court that the customer had acted negligently by allegedly keeping the PIN together with the stolen and misused bank card. To support its position the bank declared that the timing between the last use of card by the client and that the misuse of the card happened within one day. The holder insisted that that he had not written down the code anywhere, because he had kept the code in memory. The client lost the case, but appealed it.

While waiting for the examination by the appeal court, Paal Øiestad received a letter from the bank where the bank offered an apology for having accused him of gross negligence by keeping the PIN together with the card. It was mentioned in the letter that bank had been informed by their sub service supplier that transactions had been executed without using any PIN, as the customer stated from the beginning. The bank refunded the losses after all.

However, in another similar Jørgensen case the victim had not received the compensation.[51] In that case, the Trondheim District court in Norway stated that a card holder acted with gross negligence based on the fact the unauthorized payment transactions on the customer's bank card were conducted in a relatively short time period (one hour) after the card was stolen. As in Øiestad case, Jørgensen insisted that the code to his card was kept in a safe in his house and not kept together with the stolen card.

Hence, another point of the negligent behavior can be determined: *if the consumer cannot prove that he did not keep the PIN and the card together in an unsecured place*, he will be liable because of his negligent behavior. Moreover, one negative aspect also should be stressed here: in the absence of reliable evidences about negligent behavior of the consumers "the courts protected the resourceful rather than the weaker party".[52]

The evaluation of the fraudulent withdrawals must be consonant with the consumer protection legal framework. The case study N 116/02 of the UK financial ombudsman can be mentioned as an example here.[53] In spite of his fact that the PIN was kept with the card, it was stressed that according to the UK Consumer Credit Act the consumer cannot be held liable for

[50] Nuth, "Unauthorized Use of Bank Cards with or without the PIN", 98
[51] Ibid, 95
[52] Ibid, 98
[53] Financial Ombudsman Service in the UK, Disputed transactions case studies, 6

unauthorised transactions made by someone who has the card without the cardholder's permission. Moreover, the ombudsman declared that the issue of whether the client had recorded PIN is irrelevant and told the bank to reimburse the losses.

To sum up, gross negligence was and remains a "concept plagued by its lack of clarity"[54] and consistency. Furthermore, any new circumstance can change the liable party in dispute, what escalates the problem. Different approach in resolving disputes is also observed in different jurisdictions, that certainly does not make the situation better for consumers.

3.1.2 The burden of proof and presumption of gross negligence: bank is always right

The burden of proof is also regarded as a challenging issue in the case of fraudulent transactions with electronic payment instruments. From the one side, consumers do not possess the necessary technical means to prove convincingly their statements. From the other side, it could be also complicated for the issuer bank to prove the negligent behavior of the card holder, when, the latter denies that he has written his personal code on a paper in his wallet.

As we observed above, in several countries (Netherlands, Germany, Norway) a presumption of gross negligence is applied. This presumption establishes the liability of the payment service user based on the fact that a third person has been able to use the instrument protected by a PIN.[55] *In other words, if the service payment provider has been able to prove that the instrument and PIN have been used, the user must prove the absence of gross negligence.*

However, in the Belgian Act of 17.07.2002, the legislator explicitly prohibited the use of presumption of extreme negligence, where the mere fact that a third person was able to use the instrument cannot prove that the holder has been negligent.[56] According to the Court of Appeal in Brussels, it is the responsibility of the issuer to provide with arguments which prove the negligent behavior or fraud of the user.[57] The same position was announced by the Dutch Minister of Finance that the burden of proof remains with the banks.[58]

Before the implementation of the PSD, the burden of proof was not explicitly determined in the Recommendation. Article 7.2 sub (e) of the Recommendation puts the burden of proof with the issuer only partially. The issuer had to provide the proof without prejudice to any

[54] van der Meulen, "You've been warned", 715
[55] Steennot, "Allocation of liability", 558
[56] Ibid, 558
[57] Ibid, 558
[58] van der Meulen, "You've been warned", 715

proof to the contrary that may be produced by the holder. However, Schudelaro stressed that the possibility for the consumer to produce counterproof is mainly theoretical.[59] Individuals often simply do not have means to obtain and present such proof in contrast to banks.

Article 59.1 of the PSD provides a more précised rule relating to burden of proof. When payment service user denies having authorised the executed payment transaction, the payment service provider has to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency.

Besides, in the second part of the article 59 legislator determines that the use of a payment instrument, recorded by the payment service provider is in itself *not necessarily sufficient* to prove either that the transaction was authorised by the payer or the payer acted fraudulently of failed with intent or gross negligence to fulfill one or more of his obligations under the article 56. The question arises whether this rule prohibits the use of a presumption of gross negligence?[60] Steennot suggested, that it was a political compromise of legislators on behalf of different jurisdictions of Member States and, at the same time, a legal ground for the courts to decide whether or not to apply the presumption of gross negligence.

Unfortunately, this approach does not add any legal clarity, particularly for consumers. Since there is no clear criteria about negligent behavior, customers stay vulnerable to unpleasant outcome in the case of fraud with their funds.

However, it does not appear to be an easy solution that would strengthen the consumer position. If the card was lost, it sounds reasonable to allocate the burden of proof on the consumer. Conversely, with regard to security procedures, such as a PIN, it is the financial institution that ought to be required to prove proper verification.[61] The idea to define gross negligence merely referring to the theft or loss of the payment instrument also cannot be entirely justified, as in many situations it can be impossible to understand whether the instrument has been lost or stolen.[62]

Therefore, due to the fact that banks have greater resources and technical capabilities including the possibility to choose the type of security level, it is suggested here that the burden of proof should be imposed upon them. Application of the presumption of the gross negligence should be limited, because the methods to obtain payments details have

[59] Schudelaro, "Electronic payments and consumer protection", 106
[60] Steennot, “Allocation of liability”, 558
[61] Geva, “Consumer liability in unauthorized electronic funds transfers”, 233
[62] Steennot, “Allocation of liability”, 558

permanently evolved and the consumer is often not ready to resist such adverse developments. Besides, non-use of this presumption would certainly encourage banks to make more investments in technological enhancements to protect clients against fraudsters.

3.2 The problems of law enforcement within the Russian Federation

3.2.1 Burden of proof in Russian case law

The Russian Federal Service for Supervision of Consumer Rights Protection (Rospotrebnadzor) stated in its report 2013[63] that the NPS law has strengthened protection of the consumer rights in the electronic payments. It was also declared that the liability for the fraudulent transactions initially transferred to the banks. Following these allegations the Russian case law will be examined to assess the efficiency of the new legislation.

First example involves the misuse of a credit card that happened with its owner from the Russian town Podolsk when two unauthorised transactions were conducted in Seoul, South Korea.[64] The plaintiff stated that she had never received a notification from the bank about these withdrawals. She also argued that in the day of debiting she was at her workplace in Podolsk and that the PIN has been securely kept. The credit card was blocked only when she requested account statement, particularly on the 15th day after withdrawals.

Contrary to the client, the bank claimed that the SMS-notification was sent to the telephone number which was designated by the customer in the application form on the issue of credit card. The court also rejected the plaintiff's argument about technical problems with receiving messages on the customer's phone. It was also pointed in the decision that the client had not tried to inform the bank about this problem. *Moreover, the plaintiff had not proved the fact that the PIN and card details were not presented to the third party.* From the foregoing, the court inferred that the transactions had been made with the client's consent. Besides, at the stage of the contract conclusion *the plaintiff agreed with the terms of use of a credit card* by signing of the application form. As a result, the fact of signing had established the client's obligation to update the contact information pursuant to article 9.1 of the NPS law.

In a similar case, the Volgograd District Court also ruled in favor of the bank.[65] The client did not provide the evidence that the withdrawal was fulfilled by the third party without her consent. Pursuant to the judgment, the argument that the plaintiff was not in the same city

[63] Rospotrebnadzor, "Consumer protection in the Russian Federation 2013", 74
[64] Moscow City Court, Appeal decision N 33-7065, 10.03.2015
[65] Volgograd District Court, Appeal decision N 33-7623/2014, 23.07.2014

where the card was debited does not exclude the possibility of obtaining the PIN and the credit card by other persons.

According to the Plenum of the Supreme Court's Resolution,[66] the burden of proof about all the requirements have been met during the execution of electronic payment transaction lies on the banks.[67] However, banks claim their counterarguments such as the obligation of the client to ensure the safety and confidentiality of his electronic signature key.[68] Unfortunately, contrary to the obvious fact that the consumers do not have the technical capabilities like the banks, Russian courts often support arguments of the operators. Moreover, the fact that the customer has been recognized as the victim in the criminal case also does not strengthen his position.[69]

Given the continuously rising speed of developments in technology, the court should force banks to provide more evidences in doubtful circumstances and to investigate thoroughly the details of fraudulent transactions. The courts also do not capture the fact that technology, no matter how sophisticated it is, may be broken by tomorrow's technology. Under these conditions customers can neither resist the fraudsters nor prove their innocence.

3.2.2 Locking consumer by contractual terms

At present, there is the increasing tendency that Russian banks bind the consumers by the contract provisions. In Voronezh, the client phoned her bank to block her credit card.[70] She explained that her wallet had been stolen while she traveled from work in a public transport. The unauthorised withdrawals had been made at 17:00 and the client's call to the bank had been done at 21:16 on the same day. The client also mentioned that she kept her PINs with her card.

According to the terms and conditions of credit cards servicing, the bank shall not be liable in the case when information about card, PIN code, control information of the client, user ID or password will be known to other persons as a result of the customer's careless storage and use. Based on this contractual term, the Voronezh District Court decided to reject the plaintiff's claim to refund losses.

---

[66] Plenum of the Supreme Court of Russia is an assembly of all the judges, which ensures the correct and uniform application of laws by the courts, and provides explanations and interpretations of the law by adopting regulations and resolutions

[67] Plenum of the Supreme Court, the Resolution N17 of 28 June 2012, RG N5829, 11.07.2012, section 28

[68] State Duma, Federal Law "On electronic signature" N 63-FZ of 06 April 2011, RG N 5451, 08.04.2011, article 10.1

[69] Moscow City Court, Appeal decision N 11-11902,16.04.2013

[70] Voronezh District Court, Appeal decision N 33-1376, 12.03.2015

Moreover, the court also established that the article 9 of the NPS law merely sets the period within which a customer must notify the bank about unauthorized withdrawal of funds. Following this point, it was stressed by the court that the article 9 does not set up the obligation to make *undeniable return* of the stolen funds if the bank was notified by the client.
In another case, the client who had tried to enter personal online banking system received several text messages for log-in and to fulfill transaction.[71] Two text messages came after a long delay from the usual bank's number. After identification, the customer received a phone call from the bank's common phone number to tell her that the online banking has a technical failure and she should log off from the system with a new code which has already come in the new text message. After she had entered the last code and came out of the system, she received a message in her browser that the system would be malfunctioning within two hours. The next day when she discovered unauthorised withdrawals, she got in touch with her bank and blocked her account.
The Novosibirsk District Court decided that the transaction was made with the consent of the customer because the user ID, permanent password and personal SMS-code were used to fulfill transaction. In addition, it was mentioned that according to the terms and conditions of using online banking *the client agreed to bear the financial risks and risks of breaches of confidentiality related to potential distortion of data during transmission via the Internet, as well as her exclusive liability for transactions made on the Internet using the received one-time password via banking services.* The client's allegation that these terms do not comply with the Russian consumer protection law[72] was not considered by the court as justified and it was held that the bank did not have to refund the stolen money to the plaintiff.
One should note that in both cases courts referred to the terms and conditions of using cards and online banking systems which originally were designed by the banks. Under these circumstances, usually the clients have only one choice to accept these terms ("take it or leave it" approach). Moreover, under the article 9.2 of the NPS law, the operator has the right to reject client to conclude the contract. As a result, customer and bank interact on the terms that are foremost convenient to the bank. Studying these cases one question appears: how could the victim of online fraud not be liable if he or she, in fact, had already accepted to bear losses from the potential distortion of information during its transmission via the Internet by signings the operator's terms of use?

[71] Novosibirsk District Court, Appeal decision N 33-2436/2015, 24.03.2015
[72] Supreme Soviet of Russia, Federal Consumer Protection Law N2300-I of 07 February 1992, RG N8, 16.01.1996

The same tendency of contractual binding in Europe was described by van der Meulen. The terms of use by the ABN Amro bank presently contain instructions as to how to improve the information security of client computers.[73] These for instance state how clients need at least antivirus software on their computers and how they must have installed all updates. Customers agree to the terms of use by opening and subsequently using the account. The author came to conclusion that this situation consequently means that if victims do not adhere to these instruction, they might be vulnerable for liability claims if they fall victim to Internet banking fraud.[74]

In fact, many of the European banks today such as the UK Barclays, Norwegian DNB, Royal Bank of Scotland offer to all online banking customers a complete and free internet security package. Nevertheless, I believe that such offer cannot be considered as the ground for the consumer liability and there are two substantial reasons for this. Firstly, experts state that thieves using the malicious software are capable of defeating multiple layers of security, including hardware tokens, one-time transaction codes and antivirus software.[75] Secondly, it is impossible to install security software on all computers which the customer uses for the execution of electronic payment transfers. In the absence of unbounded access from different places the stated purpose of electronic payments would be undoubtedly lost.

In the end of this section, it should be noted that the client's presumption of innocence declared by the NPS law has very poor effect. As it was mentioned before, the Voronezh District Court stated that the return of the stolen funds in the case when the bank was notified by the client is not undeniable. This authoritative claim makes the position of the consumers potentially weaker. However, one should admit that "the inclusion of more specific terms of use can potentially reduce the lack of clarity and consistency, since banks are more transparent about their expectations."[76] One main concern is whether the customers would read and follow the terms and whether the banks would establish the terms that will meet not only their commercial interests.

3.2.3 Legal gap in the Russian legislation

It is not clear how the NPS law distinguishes the actions of conscientious users who have become victims of professional scammers and users who operate fraudulently.

[73] van der Meulen, "You've been warned", 715
[74] Ibid, 715
[75] See online at: http://krebsonsecurity.com/2012/07/eu-to-banks-assume-all-pcs-are-infected/
[76] van der Meulen, "You've been warned", 716

To illustrate, in one case, the client filed a lawsuit against his bank to protect his consumer rights.[77] The problem appeared when the plaintiff tried to log in his online banking. When the client has entered the password, an error occurred. In the same time customer received a phone call from the telephone number which was indicated as one of the phones of the bank. After a conversation a notification has come to his cell phone about the withdrawal. When the client applied to the bank about return of a sum of the withdrawal, the bank's employee reported that the funds were transferred to the account of a third person S. The defendant claimed that the transaction was confirmed by entering the correct code and the client also used the proper login and password to enter online banking.

During the court proceedings several facts have been determined which pointed to friendly fraud character of this case. Firstly, the plaintiff noted that the transaction was conducted from another IP-address which did not match with his IP-address when he tried to log in. Secondly, the plaintiff had not saved the text message with the code in the phone memory. Thirdly, he presented the photos with the information which appeared on the monitor of his computer during the moment of fraudulent act. These photos did not match with the official website of the bank. All these arguments, as well as the presence of a third party S. with whom the plaintiff was allegedly unfamiliar, consistently raise doubts about the innocence of the customer.

However, in spite of this fact that the client has not been refunded by the bank, there is no clarity how the friendly fraud cases should be assessed in the court. The absence of the same regulation like in Europe when the client is liable for unauthorized transactions within €150, as well as reference to the possible fraudulent client's actions which were stressed in the Article 61 of the PSD, is an obvious drawback of the Russian legislators. Furthermore, experts point out that this legal gap encourages customers to misbehavior.[78]

From the foregoing, it is suggested that the NPS law actually puts on the same level real fraudsters and ordinary users who could not resist the attacks of the perpetrators. In practice, the operators need only the fact that the correct PIN and card details have been entered. After such control activity, the customer simply becomes an abuser of the terms of use, and is, therefore, held liable for the unauthorised transaction. Thus, the concept of notification eventually has no meaning for the purposes of detecting liability in such situation.

[77] Omsk District Court, Appeal decision N 33-2622/2015, 29.04.2015
[78] Gorovcova, "Refund for unauthorized transactions", 5

The similar problem within the EU was also discussed by Steennot. He mentioned that according to the Belgian Act of 2002 it is determined that the payment service user cannot be held liable when an unauthorised person used the instrument fraudulently without physical presentation or electronic identification of the instrument.[79] However, the Directive also does not contain such bright lines rule. To determine liability of the user the payment service provider shall prove that transaction has been authenticated (article 59.2 of the PSD). According to article 4.19, authentication means a procedure which allows the payment service provider to verify the use of a specific payment instrument, including its personalized security features. If the transaction was executed with the use of the credit card number and its expiry date it could be argued that *this information does not constitute personalized security features.* This approach can reduce the liability of the consumer when someone else has used his credit card details to pay for goods and services at a distance, since the payment service provider will not be able to prove that the transaction was authenticated.

3.3 Findings of the Third Chapter

Drawing the conclusion to this chapter, one should admit that the liability regime established by the Russian NPS law gives the benefit to the operators, but not to the customers. Under these circumstances all clients irrespective to fact of notification and their real intentions will be held liable for the withdrawals which were made with correct PIN, personal password and card details. Unfortunately, this approach understudies the European conception of gross negligence. The existing case law clearly points out the legal gap and the necessity of further improvement of the current legislation. Contractual binding inherent in the recent banking practices must be avoided and punished. The negative law enforcement should be reconsidered: the obvious failure of the consumer to prove the facts of the fraud committed by third persons should not be a decisive factor in rendering of decision.

In EEA, the question of negligent behavior remains the potential challenge. Courts of different countries make different decisions under equal circumstances of the case. The lack of clarity in the Directive and different approach in assessments of the facts spoil the situation for the consumers. The primary attention should be devoted to the UK law enforcement, where consumer rights are of paramount importance to the circumstances of the case.

[79] Steennot, "Allocation of liability", 558

4. Suggestion for alternative approach to loss allocation issue

The diversity of legal systems gives the opportunity to compare above-mentioned liability regimes with the regulation of loss allocation in other countries. Undoubtedly, that the large US experience in this question is indispensable in the examination of the loss allocation issue. Moreover, this chapter will assume the price of the electronic payment fraud. This will allow looking at the problem from a different angle to find the optimal regulation rules for the participants of the electronic payment transaction.

4.1 The liability regime in the United States

The problem of payment card fraud and subsequent allocation of financial losses has a great relevance in the United States also. American authors stress that the payment card fraud entails not only the increasing payments costs, but socialized losses as a result of the law enforcement recourses spent combating this problem.[80] The optimal level of loss allocation rules helps to ensure a social welfare standpoint and facilitate commerce by limiting the cost of payment transactions.

The allocation of liability in the US occurs through a combination of public law and private ordering.[81] The public law regulation is presented by the Electronic Funds Transfer Act (EFTA) of 1978 and the Truth in Lending Act (TILA) of 1968, which determine radically different approach to deal with the liability's issue.

The EFTA is implemented through Regulation E and applies to electronic fund transfers, i.e. any transfers of funds which are initiated through an electronic terminal, telephonic instrument or computer (including online banking) or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. Hence, transfers of funds originated by check, draft, or similar paper instrument are not covered by the EFTA (12 CFR 1005.3(c)). Furthermore, the EFTA can only be applied if a transaction is initiated by the consumer who holds an account primarily for personal, family, or household purposes.

The EFTA establishes consumer's liability for unauthorised transfers (12 CFR 1005.2(m)) and transfers which were initiated by other than the consumer person, provided with the access device by the consumer. Therefore, the consumer will be liable for all types of transactions

[80] Levitin, "Private disordering? Payment card fraud liability rules", 3
[81] Ibid, 3

that have been fulfilled, but in the case when the transaction is unauthorised the liability of the consumer will be limited.

In the case of unauthorised transactions, the following procedure applies (12 CFR 1005.6). If the loss or theft of the access device is reported within two business days after learning, the maximum liability will be only up to a value of $50 or the amount of unauthorised transfer (whichever is lesser). If a consumer fails to notify the institution within two business days after learning of the loss or theft of the access device, the consumer's liability cannot exceed $500. Consumer will be liable for all transactions if he fails to report within 60 days of the transmittal of the periodic statement, on which the unauthorised transfers are recorded. For such transfers occurring after the 60-day period, liability will be unlimited until the consumer notifies the financial institution. Moreover, the financial institution may impose less consumer liability than described above based on state law or the deposit agreement (12 CFR 1005.6(b)(6)). The time limits can be delayed for extenuating circumstances, such as extended travel or hospitalization (12 CFR 1005.6(b)(4)).

According to EFTA regulation, the extent of the consumer's liability is determined solely by the consumer's promptness in notifying the financial institution. Following this point, one has to look only at the timeframe of the notification. Other additional elements such as the consumer's negligence or an agreement between bank and client which provides for the greater liability are prohibited.

However, these rules only apply if the financial institution has provided the disclosures required by the EFTA and if the access device is an accepted access device (12 CFR 1005.2). Furthermore, the financial institution has to provide a means to identify the consumer to whom the instrument was issued, for instance, it can be personal identification number (12 CFR 1005.6(a)). If one of these conditions is not met, the holder cannot be held liable at all.[82]

The TILA applies to credit cards with intention to ensure that credit terms are disclosed in a meaningful way so consumers can compare credit terms more readily and knowledgeably. This act protects individuals against inaccurate and unfair credit billing and credit card practices and contains more favorable liability regime for the card holders. Once notification has taken place, the holder of a credit card can no longer be held liable. For transactions that have been executed before notification, the liability of the holder will be always limited to $50. In addition, this regime is irrelevant as whether the holder acted extremely negligent so to the timeframe within the holder has notified the bank.

[82] Steennot, "Allocation of liability", 560

4.2 Zero liability policy as an alternative regulation

The liability for unauthorized transfers in the US is regulated not only by the federal law. According to Florencio, federal "regulation governs banks, brokerages, and credit unions, and many organizations go beyond it and offer consumers a zero liability policy,"[83] which implies a full reimbursement of bank account for any losses due to unauthorized activity. Furthermore, Epstein and Brown state that there is no reason to restrict the consumer liability for unauthorised transactions by statue at all. "If payment card companies think larger penalties are appropriate and disclose such penalties to consumers, the losses should not be socialized as a matter of law."[84]

One should note that many of American banks, MasterCard and Visa apply so-called zero liability policies that often reduce consumer liability beneath the federal liability cap.[85] These caps essentially set up a negligence regime until the level up to $50, after which the rules of federal regime take over. In other words, "market pressures have pushed the balance still further, insulating payment card users from essentially all fraud losses."[86] As a result, Levitin concluded that "the federal law is unnecessary (but fortunately harmless) intervention."[87]

Following this statement, Levitin argues that the mandatory federal rules "create a moral hazard and effectuate a wealth redistribution from consumers who engage in low-risk behavior to consumers who engage in high-risk behavior."[88] As a consequence, under the limit up to $50 consumers has become indifferent for to control their transactions and cards.

Additionally, there is high risk that customer can transfer his money to another account which is also controlled by him and claim after about fraud demanding to refund the amount of "stolen money". In this situation only bank itself can understand the client's goals and does not repudiate fraudulent remittances.

On the other hand, without the mandatory caps, the zero liability policies might not acknowledged. Adverse selection, disproportionate negotiation costs, information asymmetries, consumer hyperbolic discounting, the relative salience of different price points

[83] Florencio, "Is everything we know about password stealing wrong?", 63
[84] Epstein, "Cybersecurity in the payment card industry", 219
[85] Levitin, "Private disordering? Payment card fraud liability rules", 40; Florencio, "Is everything we know about password stealing wrong?", 63
[86] Epstein, "Cybersecurity in the payment card industry", 219
[87] Levitin, "Private disordering? Payment card fraud liability rules", 40
[88] Ibid, 40

to consumers, and consumers' limited ability to absorb losses relative to other payment card network participants - all militate for capping consumer liability.[89]

Besides, the American banks supposed that passing the liability to consumers would have more negative consequences than advantages which banks get from intensive using their financial services. Presumably, zero liability policy offered by the banks and considered as a guarantee to clients allows keeping losses more manageable contrary to the enormous efforts to save security and privacy of the clients.

It is undeniable that the guarantee provided through zero liability policy potentially diminishes the financial risks for the one individual and precludes the uncertainty for the customers. Notably, that the US approach was also admitted by the Reserve Bank of India and the House of Lords Science and Technology Committee in the United Kingdom.[90] Similarly to the American banks, most major Canadian banks offer a 100% reimbursement guarantee for online banking fraud losses.[91] This popularity indicates that in spite of the possible negative impact on the consumer's behavior, the adoption of zero liability can tackle the loss allocation problem with more efficiency. In other words, by applying this policy US banks offer the upper bound of the consumer protection, actually exempting them from liability in the case of unauthorised transfers.

4.3 The price of electronic payment fraud

Generally speaking, the consumer should feel himself most comfortable under the zero liability regime, since he is largely isolated from the financial consequences of the fraud. Nevertheless, the fraud costs are part of pricing[92] and the question about covering losses is still remained urgent.

Payment card transactions include multi-party networks of financial institutions, consumers and merchants. Transmission of money from a consumer to a merchant for paying goods or services is conducted through the consumer's bank (the issuer bank), the merchant's bank (the acquirer bank) and the card network association (MasterCard, Visa) that intermediates between the banks and sets the rules governing their transactions. In a payment card transaction, the consumer must first transfer information about consumer's account to the merchant's acquirer or data processor.

---

[89] Ibid, 40
[90] van der Meulen, "You've been warned", 717
[91] Florencio, "Is everything we know about password stealing wrong?", 63
[92] Levitin, "Private disordering? Payment card fraud liability rules", 8

By the merchant's processor the information is relayed to the credit card network for authorization, capture and settlement. Authorization involves the card network first verifying that the card is real and then the issuer approving the transaction. Once a transaction has been authorized, it may then be captured.[93] When the transfer of funds is conveyed from the issuer bank to the acquirer bank, the network debits the issuer's account for the amount of the transaction less the interchange fee and credits the acquirer bank's account for the transaction amount minus both interchange and network fees. Finally, the merchant gets the transaction amount minus merchant discount fee which consists of interchange and network fees paid by the acquirer. The card network also takes out various fees to cover the processing costs plus its profit margin.

A central role of the network association is to coordinate optimal participation in the network through price manipulation and the networks rules that impose the liability on the network participants for losses or limit network participant's ability to reallocate costs to other network participants.[94] Eventually, the cost of fraud is also included in the total price of participating in a payment card network and merchants as the consumers certainly pay these costs. However, it makes sense between to be personally liable for losses and to share losses that are distributed among all users of the payment chain.[95]

Historically, in the CNP payment chain merchants decided that the gains from these transactions outweighed the fraud risks, so they agreed to assume liability for unauthorized mail-order and telephone-order transactions.[96] Moreover, earlier merchants could always control risks by cancelling of the delivery of the goods before receiving and verification of a paper check. However, with a huge growth of electronic transactions via Internet this option was nullified for them. Today, payment networks and/or issuers require payment details, verify the information and, as a result, can prevent fraud.

The issuer can always enhance the security level for the electronic transaction by widening the requirements for its execution: not only the card account data and the card verification value (CVV) can be requested, but also the billing address, telephone number, e-mail address information. All these details can be verified by the issuer with the information supplied by the client and supplied to the merchant to ensure that account and initiator are real. Furthermore, the issuer can use statistical fraud prevention tools called *neural networks* that

[93] Ibid, 11
[94] Ibid, 14
[95] Florencio, "Is everything we know about password stealing wrong?", 63
[96] Levitin, "Private disordering? Payment card fraud liability rules", 20

can identify anomalies in spending behavior by analyzing transactions in relation to the cardholder's transaction history, looking for outliers in geography merchant type, and transaction amount.[97]

However, the end-users of the payment network can always choose the level of protection or the method of verification. As the consumer can confirm the transaction by the filling of the PIN or putting signature on the receipt, as well the merchant can choose the type of verification of the electronic payment. In fact, the merchant considers various factors to find the balance between the cost of fraud, fees for using payment services and the effect of the e-commerce: if the verification would be too complicated for clients, it can reduce the volume of sales; if the acquirer bank acts as the issuer bank, the interchange fee is excluded and the cost of the payment will be reduced.[98] Thus, the merchant can calculate all charges and lay them in the price of goods or services.

Nevertheless, the role of issuers and the card network associations is the core in the electronic payment transactions. Usually, it is the issuer bank which on default selects the type of verification for the clients and it is the card network association which sets prices and rules for allocation of losses. That is why only placing the liability on these payment conductors would encourage them to undertake greater security efforts to avoid the fraudulent withdrawals. From the foregoing, forcing consumers to pay for unauthorised transactions should be considered as the failure of the payment architecture for which the developer should be responsible and not the consumer.

4.4 In the quest of the optimal regulation

Both the European and US liability regimes have similar rules regarding transactions that have been taken place after notification. However, the approach is totally different when it comes to liability for transactions that have been executed before notification. The problem with the European approach is that the concept of gross negligence plays a too important role. [99] "Allocating liability for fraudulent transactions that have taken place before notification exclusively in function of gross negligence implies that the burden of proof will

[97] Ibid, 22
[98] Polozov-Jablonskiy, "Air ticket online"
[99] Steennot, "Allocation of liability", 560

in reality, at least in many cases, determine the extent of liability."[100] The ambiguity of the rule relating to the burden of proof, which is established in the article 59.2 of the Directive leads to unjustified results of the cases with the similar conditions.

From the one side, if the European legislators would have clearly imposed the onus of proof on the client, the limitation of liability would have been purely fictitious, because a payer will practically never succeed that he did not act negligently. From the another side, explicit prohibition of the presumption of gross negligence would create too many cases where the payment service provider is liable for all transactions exceeding €150 in situation of failure to prove the existence of gross negligence.

Steennot states that the conception of the gross negligence should be changed but not eliminated. More specifically, the liability of the payment service user should be determined in function of the timeframe within which the payer notifies the payment service provider of loss or theft, which establish that a late notification as such cannot constitute gross negligence.[101] It can guarantee that the liability of the payment service user who did not act negligently and who notifies the provider in time limited. Moreover, Steennot argued about several benefits for the system, particularly, the possibility to be liable will stimulate consumers to keep their cards safe and to notify loss or theft the providers as soon as possible.

Undoubtedly, that the European liability regime keeps the consumer in good shape avoiding the full responsibility of the providers. However, this advantage seems to be a dubious achievement in a broad sense. The conception of zero liability excludes risks for the consumers. Since the consumer feels himself more secure, he is ready to use his payment instruments more often what gives additional growth impact to economic development. Another good thing is in decreasing of the judicial system costs. If the disputes between users and providers would appear less often, the courts would spend less time for to resolve them. It, certainly, can benefit the economy and society in whole.

The Russian approach to allocation of losses differs from the European and US regimes. In spite of this fact that the Russian legislators steadily state about the commitment to the European legislation, the NPS law established other rules to liability in the case of unauthorised transaction. Here the notification should be done by the both parties: first, the operator should notify the client about the transaction and, then the client should notify the

[100] Ibid, 560
[101] Ibid, 560

operator about the transaction which had been executed without his consent. However, devil is in the details.

First, the client has very limited time frame for sending such notice which does not account life circumstances (e.g. illness, vacation). Secondly, the operators fully enjoy the benefits from the provision of article 9.15 of the NPS law. In most cases, banks simply claim that the customer has violated the order of use of the payment instrument, what gives them an unlimited right not to refund the losses.

Critically, the current mechanism is useless in many cases of online scams and phishing, where the clients themselves provide the fraudsters with passwords and PIN codes. According to the Russian case law, if the transaction was executed with the correct PIN code and private password it is automatically makes the client liable. Thus, the correct PIN code is considered as a direct violation of the use of the payment instrument by the client.

Finally, the lack of legal clarity about agreement's conditions and the form of notification also gives rise to extensive litigation, whereas the courts make decisions on a case-by-case basis.

In contrast to the banks, the customer has a very small chance and technical resources to prove the fault of the fraudsters. However, in most of the cases courts impose the burden of proof on the consumers. All these weaknesses clearly emphasized the necessity of further legal improvements for the relatively young Russian liability regime. Personally, in a serious lack of financial literacy among Russian citizens[102] I find the US zero liability policy the better alternative to allocate the losses. Moreover, the absence of provision which imposes the maximum of the financial loss within $50 or €150 leads to a lack of adequate allocation of fraudulent costs under any circumstances and make the consumers weaker. As a result, suffer not only the clients: all payment system, the Russian state and economy are deprived the further development, decrease of the use of cash and rise of the consumer trust to the electronic payment services.

To conclude, it is suggested here that the consumer should bear the losses only when the he was sufficiently identified during the execution of payment transaction. It means that if the transaction has been initiated by an unauthorised person transmitting the card number and expiry date of a credit card and withdrawal has been done without the consent of the payment service user, the payment service user should not be held liable. It is the responsibility of the issuers to arrange proper verification mechanisms and to develop security systems. General

[102] Klapper *et al.*, "Financial literacy around the world", 24

use of such types of protection and proper control of the electronical payments should be an indispensable condition in consumer servicing.

5. Demand for revision and better security

The inevitable development of the technology leads not only to enjoyment by its benefits, but to the need of law updating. Moreover, the identification of existing problems provides additional boost for legal changes. According to Impact Assessment[103], the European payment market has several issues such as inconsistent application of the existing rules across Member States, lack of standardization and inter-operability between different payment solutions, security and trust flaw, etc. Since the Russian NPS law is relatively new framework for significant changes, the next chapter is mainly dedicated to the European regulation. However, the study of the coming improvements on the European payment market can be certainly helpful for the Russian legislators too.

5.1 The revision of the current European payment regulation

On 24 July 2013, the European Commission adopted a proposal for regulation payments within the European Union, i.e. a revised Payment Services Directive (PSD2) and a Regulation on Multilateral Interchange Fees (MIFs).[104] The need of legal modernization was prompted by the growing number of credit and debit card payments, the rise of e-commerce, substantial growth of internet and mobile payments and the emergence of new means of payment (e.g. smartphones). In this context, the PSD2 determined the main goals: to help develop further market for electronic payments, which will enable consumers, retailers and other market players to enjoy the full market's benefits and to promote more competition, efficiency and innovation.[105] To achieve these objectives the market should function in a legal clarity and transparency of payment services. As a result, the Proposal will repeal the current PSD and introduces changes for the better consumer protection against fraud and payment incidents.

According to the summary of the main modifications, the liability rules in case of unauthorized transactions will continue their harmonization and the enhanced level of

[103]European Commission, Commission staff working document. Summary of the Impact Assessment, 3

[104] See online at: http://ec.europa.eu/finance/payments/framework/index_en.htm

[105] European Commission, the Proposal on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Context of the Proposals, Grounds for and objectives of the proposal, 24.07.2013

protection of the legitimate interests of the participants will be ensured. For example, article 66 of the Proposal decreased the maximum amount of payment when user could under any circumstances be obliged to pay in case of unauthorized transaction from €150 to €50, except in case of fraud and gross negligence.

For reducing the risk of fraud, especially in the online payments, and to protect confidentiality, the above-mentioned article also presents a new interesting provision:[106]

> For payments via a distance communication where the payment service provider does not require strong customer authentication, the payer shall only bear any financial consequences where having acted fraudulently. Should the payee or the payment service provider of the payee fail to accept strong customer authentication, they shall refund the financial damage caused to the payer's payment service provider.

More specifically, article 4.22 of the PSD2 determines the stricter approach to security: contrary to the simple authentication strong authentication is based on the use of two or more elements categorized as knowledge (something only the user knows, e.g. a password or PIN), possession (something only the user possesses, e.g. the card or authentication code generating device) and inherence (something the user is, e.g. fingerprint or voice recognition) to validate the user or the transaction.[107] These elements are independent (the breach of one element does not compromise the reliability of the others) and designed in such a way as to protect the confidentiality of the authentication data.[108]

The use of biometric data (inherence element) for banking services is the most controversial aspect. The storing client's sensitive information in databases could be risky because it would attract criminals and, to a certain degree, would create a fear of losing privacy among the clients. Moreover, the financial institutions would have to invest more money for development of new security measures, what finally would lead to the rise of the costs of payment services.

However, the Commission points that it is not always necessary and convenient to request the same level of security from all payment transactions. The Commission together with the European Banking Authority will adopt the exemptions to the principle of strong authentication (e.g. low value payments at the point of sale), taking account of the risk involved, the value of transactions, channels used for payments, etc.

---

[106] European Commission, the Proposal on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, 24.07.2013, article 66.1

[107] European Commission, "Payment Services Directive: frequently asked questions" 08.10.2015, question N16

[108] Ibid, question N16

Nevertheless, the legislator has not changed the article 59.2 of the PSD with the ambiguity provision about who has to prove the absence or existence of gross negligence. However, according to new provisions, if the amount of transaction would be reasonable, it would be consistent to establish strong authentication for payments on the distance. Presumably, in the case of strong authentication the question about negligent behavior ceases to be the problem for the customers.

Moreover, the revised Directive provides "a stronger position in case of disputes with their bank and other payment service providers: the new rules will oblige banks to answer in written form to any complaint within 15 business days."[109] The Member States will be obliged to qualify competent authorities to work over complaints of payment service users and other concerned parties, such as consumer associations. Payment service providers in their turn should put in place a complaints procedure for consumers that they can use before seeking out-of-court redress or before launching court proceedings.

Generally, the PSD2 makes a huge step towards the consumer. In spite of this fact that the gross negligence approach has not been excluded, the provision about strong authentication sounds like a grave effort to protect users from fraudsters. It is obvious, that the criminals will develop new ways to seize other people's money, but it is also obvious that only issuers and card network associations can resist them and protect the client's accounts.

5.2 Additional legal means for prevention of losses

The article 55.1 of the PSD has an important provision about limits of the use of the payment instrument, which can serve as an additional method for the protection of the consumer's funds. By establishing the agreement on spending limits for payment transactions between the client and the bank, the parties can secure themselves against reasonable amounts of losses (e.g. limiting the amount that can be debited in one week or per month). Following this provision, one of the major advantages of spending limits is that consumers cannot be held liable for the transactions, exceeding the given spending limits and finally avoid losses.

Moreover, the article 55.2 of the PSD establish the right of the payment service provider to block the payment instrument for objectively justified reasons related to the security of the instrument. The provider's right to block should be agreed in the framework contract. However, before blocking the instrument the bank must where possible inform the holder of

[109] European Commission, "Payment Services Directive and Interchange fees Regulation: frequently asked questions" 24.07.2013, point B, 4

the payment instrument in order to verify whether fraud has taking place (article 55.3). Such blocking can also bring negative consequences in some situations: if the payment instrument was not stolen, lost or used fraudulently the customer may be severely constrained, for instance, during the vacation abroad. However, the payment service provider will only be liable if it did not make a *bona fide* effort to contact the payment service user before blocking the instrument or if normal payment service provider acting with reasonable care would not have blocked the use of the instrument, because the spending pattern did not justify the suspicion of fraudulent use.[110] The blocking alternative can be helpful for the clients with credit lines: such right could stop fraudulent transfer and help to avoid paying debts and interests.

Notably that both provisions has been also included in the revised Directive (article 60). Unfortunately, the Russian NPS law does not contain such simple but important measures. Instead of this, the banks offer a chargeable insurance for the cardholders where the bank can reimburse the financial losses within the amount of the insurance coverage.[111] Obvious, that the insurance claims do not cover all types of fraud with electronic instruments: refunding is stipulated only in the case of cash theft within 2 hours after removing card from ATM or the card theft and card loss. Ultimately, the efficiency of such protection is extremely doubtful and leads to additional and worthless costs instead of agreement about spending limits.

Hence, one can admit that regulation of the electronic payments in Russia is not sufficiently developed in comparison with the EU and US. The liberty of the Russian banks based on the freely designing terms of use of electronic payment instruments together with the current case law in their favor, gives them assertive ability to deny refunding losses. Therefore, the promotion of limits can certainly change the situation in a better way, suppressing the possibilities of the fraudsters and placing full liability on the banks.

[110] Steennot, "Allocation of liability", 559

[111] See online at: http://www.sberbank.ru/ru/person/bank_inshure/insuranceprogram/cardholder/faq

6. Conclusion

Fraud with electronic payment instruments is harmful to all participants of the electronic payments except the perpetrators, but it is clear that the consumer is the weaker party in the unauthorized payments. Hence, I believe that the law should protect the consumers and limit their liability when the question of loss allocation occurs.

Both the European Payment Service Directive and the Russian Law On the National Payment System have created the liability regimes to regulate the fraudulent electronic payment transactions. Unfortunately, these legal frameworks have serious weaknesses (e.g. the presumption of gross negligence and late notification in Europe, limited timeframe for notification in Russia, etc.) which do not allow strengthening the position of the consumer. From the observed case law one can admit that the laws are ineffective and the courts are deaf to the consumers who mistakenly provide the fraudsters with PIN or private passwords. Moreover, in Europe the decisions can be controversial under the same circumstances: the approach to determine liable party depends on issuer bank of the electronic payment instrument or the court of the Member State, where the unauthorized withdrawal took place.

In Russia the banking activity is poorly controlled: clients often sign one-sided terms of use of electronic payment instruments trusting the banks. Such terms make them initially liable for fraudulent actions to which, in fact, a common user cannot resist. Consumer compliance with such terms makes banks "untouchable" in the court. The European concept of gross negligence is also applied: the correct PIN and password indisputably represent the full responsibility of the consumer. As in Europe, Russian customers have a little opportunity to prove correct use of payment instruments while banks have enough resources and technical opportunities to argue.

In the same time, in contrast to European and Russian legal frameworks, the United States offer a different approach to loss allocation issue. The private regulation is applied: zero liability policy eliminates the liability of the consumers for any losses in the case of unauthorized transactions. Furthermore, the American consumer is additionally protected by the public law which established the maximum limit of liability within $50. Since the U.S. banks and card payment associations put the number of customers and client's trust on the first place, they are ready to pay for losses.

Frankly speaking, I find the US zero liability approach as the most comfortable regime for the all participants. Since the losses from fraud with electronic payment instruments can be calculated and included in the price of electronic financial services and merchant's goods,

why the consumers have to take private liability for such losses? Why the consumers have to take a court litigation to prove that they are victims of the fraud under such circumstances when the payment networks are not enough secure and the law is inconsistent?

Nevertheless, the European and Russian legislators seem not to support the zero liability policy. In the revised Directive (PSD2) the most controversial provisions remained unchanged. However, the European Commission increased security requirements for execution of electronic payments and reduced the liability limits. The effectiveness of these provisions will be assessed later: the substantial growth of the use of electronic payments and the future development of e-commerce are the main goals of the revised Directive.

Concerning the Russian situation, the current legal framework requires an obvious mitigation in consumers favor. Personally, in the situation when the Russian people have a low level of financial and computer literacy, I find zero liability approach as the best solution of the loss allocation issue for my native country.

The European legislators send a concrete signal: the security of the electronic payments should be enhanced. Presumably, Russia will choose the same direction. However, looking to the future, one must pay attention to the following assumptions: new security measures require large financial investments, what may lead to reduced competition and negative impact on the e-commerce market; since the presumption of gross negligence continues to act, the courts should pay particular attention to the circumstances of fraudulent withdrawals and to remember about different financial and technical capabilities of the client and the bank. In other words, every consumer deserves equal and fair protection by the law.

Acknowledgments:

I would like to express my gratitude to everyone who supported me throughout the Master's program Information and Communication Technology Law at the University of Oslo. I thank my friend Ulugbek Abdullaev for his critical point of view, and my research supervisor Professor Olav Torvund for comments that helped me improve the paper.

7. Table of reference

Articles, Books, Reports

Aleshkina, Tatiana. “The Bank of Russia disclosed the volume of fraudulent transactions of Russians in 2014.” RBC Finance (2015) http://www.rbc.ru/finances/23/06/2015/558936aa9a79477bdc5736ec

Anderson, Ross, Barton, Chris, Böhme, Rainer, Clayton, Richard, van Eeten, Michel J. G., Levi, Michael, Moore, Tyler, Stefan Savage. “Measuring the Cost of Cybercrime.” In The Economics of Information Security and Privacy, edited by Rainer Böhme. 265-300. Berlin: Springer, 2013

Bank of Russia, the Survey about unauthorized money transactions 2014 (2015): 1-17 http://www.cbr.ru/psystem/P-sys/survey_2014.pdf

Barker, Katherine J., D'Amato, Jackie and Paul Sheridon. “Credit card fraud: awareness and prevention.” Journal of Financial Crime 15, 4 (2008): 398-410 http://dx.doi.org/10.1108/13590790810907236

Bhattacharyya, Siddhartha, Jha, Sanjeev, Tharakunne, Kurian and Christopher Westland. “Data mining for credit card fraud: A comparative study.” Decision Support Systems 50, 3 (2011): 602-613 doi:10.1016/j.dss.2010.08.008

Bolton, Richard J., Hand David J. “Statistical Fraud Detection: A Review.” Statistical Science 17, 3 (2002): 235-255 http://dx.doi.org/10.1214/ss/1042727940

Brignall, Miles. “Now banks are trying to pin the blame for card fraud on you.” The Guardian Money (04.05.2012) http://www.theguardian.com/money/2012/may/04/banks-pin-card-fraud

Chirkov, Aleksej. "Problems of realization of legislation on national payment system with regard to responsibility of banks in settlement legal relations." Bankovskoe pravo 5 (2013): 63-68

CRID, University of Namur and the IT Law Unit, Centre for Commercial Law Studies, Queen Mary University of London. Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer (2001):1-89

Epstein, Richard A., Brown, Thomas P. “Cybersecurity in the payment card industry” The University of Chicago Law Review 75, 1 (2008): 203-223 http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2347&context=journal_articles

European Central Bank, The Fourth report on card fraud (15 July 2015): 1-27 https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

European Commission, “Payment Services Directive and Interchange fees Regulation: frequently asked questions” (24.07.2013) http://europa.eu/rapid/press-release_MEMO-13-719_en.htm

European Commission, Commission staff working document. Summary of the Impact Assessment (24.07.2013):1-8 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0289&from=EN

European Commission, Communication from the Commission to the Council and the European Parliament concerning a New Legal Framework for Payments in the Internal Market. Consultative Document. (02.12.2003):2-72 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52003DC0718

European Commission, Payment Services Directive: frequently asked questions (08.10.2015) http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm

Farivar, Cyrus. “Clients, not banks, liable for losses in phishing scams, court rules.” Ars Technica (2012) http://arstechnica.com/business/2012/04/clients-not-banks-liable-for-losses-in-phishing-scams-court-rules/

Financial Ombudsman Service in the UK, "Disputed transactions case studies." Ombudsman news 116 (2014): 1-20 http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/116-disputed-transactions.html

Florencio, Dinei, Herley, Cormac. “Is everything we know about password stealing wrong?” Security & Privacy, IEEE 10, 6 (2012): 63-69 doi:10.1109/MSP.2012.57

Geva, Benjamin. “Consumer liability in unauthorized Electronic Funds Transfers.” The Canadian business law journal 38 (2013): 207-281 http://heinonline.org/HOL/Page?handle=hein.journals/canadbus38&div=14&g_sent=1&collection=journals

Gorovcova, Margarita. “Refund for unauthorized transactions: what will change from January 1, 2014.” Garant.ru (2013) http://www.garant.ru/article/507445/

Janczuk, Agnieszka. “The single payments area in Europe.”Columbia Journal of European Law 16 (2009-2010): 321-335

Klapper, Leora, Lusardi, Annamaria and Peter van Oudheusden. "Financial literacy around the world: Insights from the Standard & Poor's ratings services global financial literacy survey." (2015): 1-27 https://www.mhfi.com/corporate-responsibility/global-financial-literacy-survey

Korotaeva, Natalya V. “Problems and development prospects of non-cash retail payments in Russia.” Socio-economic processes and phenomena 12, 046 (2012): 166-173 http://cyberleninka.ru/article/n/problemy-i-perspektivy-razvitiya-v-rossii-beznalichnyh-roznichnyh-platezhey

Levi, Michael. “New Frontiers of Criminal Liability: Money Laundering and Proceeds of Crime.” Journal of Money Laundering Control 3, 3 (2000): 223 – 232 http://dx.doi.org/10.1108/eb027233

Levitin, Adam J. " Private disordering? Payment card fraud liability rules." Financial and Commercial Law 5 (2011):1-48 http://ssrn.com/abstract=1570867

London Economics and iff in association with PaySys. “Study on the impact of Directive 2007/64/EC on payment services in the internal market and on the application of the regulation (EC) NO 924/2009 on cross-border payments in the community.” (2013): 1-311

Mercado-Kierkrgaard, Sylvia. “Harmonising the regulatory regime for cross-border payment services.” Computer Law & Security Review 23, 2 (2007): 177-187 doi:10.1016/j.clsr.2006.11.003

Nuth, Maryke S. “Unauthorized Use of Bank Cards with or without the PIN: A Lost Case for the Customer.” Digital Evidence & Electronic Signature Law Review 9 (2012): 95-101 http://dx.doi.org/10.14296/deeslr.v9i0.1997

Obaeva, Alma S. "National payment system: infrastructure, innovation, development prospects." Dengi i kredit 5 (2010): 34-40 http://www.cbr.ru/PSystem/analytics/NPS.pdf

Polozov-Yablonsky, Andrei. “Air ticket online.” (01.03.2008). http://www.ato.ru/content/aviabilet-v-internete

Rospotrebnadzor, State report “Consumer protection in the Russian Federation 2013.” (2014):1-224 http://rospotrebnadzor.ru/upload/iblock/037/gosudarstvennyy_doklad_zashchita_prav_potrebiteley_v_2013_godu.pdf

Schudelaro, Ir. A.A.P. “Electronic payments and consumer protection: should Recommendation 97/489/SC be replaced with a Directive.” Computer Law & Security Review 17, 2 (2001): 105-109 doi:10.1016/S0267-3649(01)00205-9

Segal, Lydia, Ngugi, Benjamin and Jafar Mana. “Credit card fraud: a new perspective on tackling an intransigent problem.” JCFL 16, 4 (2011): 743-781 http://ir.lawnet.fordham.edu/jcfl/vol16/iss4/2

Staschen, Stefan. "Financial Inclusion and Innovation in Russian Payment Systems." CGAP (2013) http://www.cgap.org/blog/financial-inclusion-and-innovation-russian-payment-systems

Steennot, Reinhard. “Allocation of liability in case of fraudulent use of an electronic payment instrument: the new directive on payment services in the internal market.” Computer Law & Security Review 24, 6 (2008): 555-561 http://dx.doi.org/10.1016/j.clsr.2008.09.005

van der Meulen, Nicole S. “Between awareness and ability: consumers and financial identity theft.” Communications & Strategies 81 (2011): 23-44

van der Meulen, Nicole S. “You've been warned: Consumer liability in Internet banking fraud.” Computer Law & Security Review 29, 6 (2013): 713-718 http://dx.doi.org/10.1016/j.clsr.2013.09.007

Wei, Wei, Li, Jinjiu, Cao, Longbing, Ou, Yuming and Jiahang Chen. “Effective detection of sophisticated online banking fraud on extremely imbalanced data.” World Wide Web 16, 4 (2013): 449-475 http://dx.doi.org/10.1007/s11280-012-0178-0

Cases

AG Kassel 16.11.1993, W.M. 1994, 2110

Brussel 27.05.2002, NjW 2003, 311, T.B.H. 2004, 158

Brussels 04.10.2005, Bank Fin.R. 2006, 148

GCB 24.09.1994, T.V.C. 1995, 183

Jørgensen v DnB NOR Bank ASA, Trondheim District Court Case N 04-016794TVI-TRON, 24.09.2004

Moscow City Court, Appeal decision N 11-11902,16.04.2013

Moscow City Court, Appeal decision N 33-7065,10.03.2015

Novosibirsk District Court, Appeal decision N 33-2436/2015, 24.03.2015

Omsk District Court, Appeal decision N 33-2622/2015, 29.04.2015

Paal Øiestad v DnB NOR Bank ASA, Oslo District Court Case, 2008

Volgograd District Court, Appeal decision N 33-7623/2014, 23.07.2014

Voronezh District Court, Appeal decision N 33-1376, 12.03.2015

Legislative acts

European Commission, Directive 2007/64/EC of the European Parliament and 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, OJ.L. 319

European Commission, Recommendation 97/489/EC of 30 July 1997 concerning transactions carried out by electronic payment instrument and In particular the relationship between issuer and holder, OJ.L. 208, 02.08.1997

European Commission, the Proposal on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, 24.07.2013 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0547&from=EN

Plenum of the Supreme Court, the Resolution N17 "Courts civil cases review on consumer protection disputes" of 28 June 2012, RG N 5829, 11.07.2012

State Duma, Federal Law “On electronic signature” N 63-FZ of 06 April 2011, RG 5451, 08.04.2011

State Duma, Federal Law “On the National Payment System” N 161-FZ of 27 June 2011, RG N 5515, 30.06.2011

State Duma, the Civil Code of the Russian Federation, N 51-FZ of 30 November 1994, RG N 238-239, 08.12.1994

Supreme Soviet of Russia, Federal Consumer Protection Law N 2300-I of 07 February 1992, RG N 8, 16.01.1996

The 90th United States Congress, the Truth in Lending Act (TILA) N 90-321 on May 29, 1968

The 95th United States Congress, the Electronic Fund Transfer Act (EFTA) N 95-630 on November 10, 1978