INTERNATIONAL PROJECT ADICAE

European cycle of Seminars against the fraud in means of payment

Challenges and solutions for consumers in fraud of means of payment

Fraud Stadistics, European Seminar in Barcelona, Survey for Consumers

Organises:

ADICAE
Association of Users Banks, Savings Banks and Insurances

With the collaboration of:

DG JUSTICE, FREEDOM AND SECURITY
European Commision

Edits:

ADICAE
Association of Users of Banks, Savings Banks and Insurances

Central Office

c/ Gavín, 12 local - 50001 Zaragoza (Spain)
Tel.: 976 39 00 60
Fax: 976 39 01 99
email: aicar.adicae@adicae.net
www.adicae.net

A-S 200108

Index

PARTE 1 - PROJECT PRESENTATION

Proyect presentation 3

PART 2 – PAYMENT METHOD FRAUD IN THE EUROPEAN UNION

Introduction. 7
Payment metod fraud in the European Union 9
Payment metod fraud in Spain 10
Internet Fraud. 11
A Study of fraud in non-cash payment methods 13
Fraud complains made to the bank of Spain. 16

PART 3 - PAYMENT METHOD USERS IN THE FACE OF E-FR@UD

Presentation 17
Cybercrime under investigation by european police forces. 27
Challenges for the goverment and legislation in the face of consumer 27
fraud in electronic commerce 33
Liability in the face of fraud, is the consumer always liable 43
Experiences panel of the partner consumer associations of the project 53
A new computer offender´s profile: Are consumers protected agains them? 59
Electronic banking, Are consumers safe? 67
Round table: conclusions on the consumer´s position in the case of fraud 75

PART 4 - CONCLUSIONS

General conclusions of the Seminars 79
Proposals to the stakeholders 81
Proposals to the stakeholders (II). 82

PART 5 - ANNEXE REGULATIONS

Provissions issued by the EU on the transparency of operations
and clients protection 95

PART 6 - ANNEXE JURISPRUDENCE

The court pass sentence on payment fraud
an analysis of legal resolutions 95

PART 1

PROJECT PRESENTATION

PROJECT PRESENTATION

ADICAE, for several years now, has been predominant in voicing concerns on a national level about the emergence of new non-cash payment methods and the dual dangers that users face:

- problems in handling and using the new methods that create mistrust and result in failure or non-use.

- the proliferation of fraud in relation to these methods of payment facilitated by a lack of security applied by institutions.

ADICAE, therefore, has proposed meeting the challenge with an ambitious European-wide project covering all the facts and issues relating to non-cash payment fraud. The main objective of Project " " is to identify the current problems faced by consumers relating to non-cash payment fraud and attempt to reduce their incidence by strengthening cooperation between users, governments and the police, in order to achieve a much higher level of security, and therefore confidence.

The project was carried out in collaboration with the European Commission Directorate-General for Justice within a framework of action to promote effective improvements for all EU citizens with regard to access to justice.

The work of the authorities is shown to be inadequate since, as it is readily admitted, the criminal is usually one step ahead of the pursuer. Moreover, since fraud targets small amounts of money, the victims are usually typical consumers and investigation is greatly hindered when, on occasions, it cannot even be considered a crime. This also means that in order to claim for such small amounts, the consumer has to take costs and time invested fully into account.

As it is clear that suppression of crime is neither the only nor the main option. Other factors come into play such as prevention through providing information to consumers, who are the main targets of payment fraud, and cooperation between all those involved to improve security and confidence in these payment methods.

Through this project, several questions that need solutions have been raised: "Are non-cash payment methods secure? What are the authorities and institutions doing to improve consumer security? What should consumers do to defend their rights? Is the problem treated in the same way in other countries?

In order to answer these questions, ADICAE has developed this project in collaboration with seven other European consumer associations in Bulgaria, Slovakia, Slovenia, Italy, Lithuania, the Czech Republic and Romania.

ORGANIZACIONES PARTNERS

ADICAE

Bulgaria: "Consumers' national Bulgarian Association (BNAP)"

Slovakia: "Consumers' national Slovakian Association (ASC)"

Slovenia: "Consumers' national Slovene Association (MIPOR)"

Italy: "Associazione per la difesa de consumatori e ambiente (ADICONSUM)"
"Movimiento Difesa del Cittadino (MDC)"

Lithuania: "Lithuanian National Consumer Federation (LNCF)"

Czech Republic: "Sdružení českých spotřebitelů (SČS)"

Rumania: "Asociatia Nationala pentru Protectia Consumatorilor si Promovarea Programelor si Strategiilor din Romania (ANPCPPS)"

PROJECT ACTIVITIES

In order to disseminate the results and ensure that consumers and interested parties receive the information, it was decided to develop the following methods:

- Judicial study
- Study-survey
- Information guide also on CD-ROM
- Website and CD-ROM prevention simulator
- Symposiums in each of the partner countries and a final international symposium in Barcelona from which a DVD was produced and its events recorded.

JUDICIAL STUDY

As a starting point for the project, it is fundamental to find out about legislation in member countries and the current situation in Spain, both in terms of legislation and unfair terms. The study also seeks to overcome the traditional fixation of considering cards the only target for payment method fraud. It is evident that cards, as a result of the numbers in existence and the volume of transactions performed, are a major source of misuse, unfair terms, causes of complaints, etc. However, this study aims to provide an integrated approach from a judicial standpoint relating to the situation of consumers when they experience fraud when making transfers, purchasing online, paying with a mobile phone or using e-banking.

Front Page of the Legislative Study

STUDY-SURVEY

An analysis of Spanish people's knowledge of non-cash payment method fraud, as well as the scale and significance of fraud in society. It was conducted by means of a field study based on a survey of consumers visiting various ADICAE offices around Spain, through the Internet and in the street with users of non-cash or electronic payment methods.

The purpose of the survey was to identify the profile of the average non-cash payment method user and assess:

- Consumer perception of the security of non-cash payment methods.
- Information provided to the user before performing a transaction.
- The degree of consumer satisfaction and the main causes of grievances and complaints.
- The degree of user adoption of new technologies, with special emphasis on the Internet use and electronic banking.
- The fraud situation in Spain, its variants and scale.

INFORMATION GUIDE

Practical material has been developed to serve as a practical introductory guide for the consumer with little knowledge of payment methods. When the consumer needs to use these methods of payment but neither the information nor instruction provided by the issuing institution is sufficient or effective, materials such as the guide can help by providing information in a simple, graphic and instructional manner about the methods, how to use them, their practicality and the most common consumer frauds, as well as advice on how to avoid them. A definitive, practical and accessible guide on payment fraud.

Front Page of the Informative Block

WEBSITE - SIMULATOR

For wider dissemination of the project and results, a website has been designed, which includes an extensive description. Located within ADICAE's home page, it has been designed to provide easily accessible information. Information can be obtained regarding existing legislation, types of fraud, interesting national and international website links can be visited or advice on the use of different methods of payment can be obtained, as well as, of course, the possibility of downloading materials.

Detail of the Simulator of Fraud CD

PAYMENT METHOD FRAUD SIMULATOR

In order for a project related to electronic payment and the Internet to coincide with the characteristics of its materials, a fraud simulator has been designed, following the traditional pattern of a two-dimensional adventure game in which a character must perform real transactions to gain the highest number of points possible. In the form of a quiz, the consumer performs transactions, obtain information and achieve objectives to be a true "good user of payment methods" and prevent the bank from attempting to attribute blame for any fraudulent transaction to which he may be subjected.

SYMPOSIUMS

Seven symposiums have been held in the partner countries, including Spain, focused on consumers and also a knowledgeable public so that there could be information exchanges and interesting and representative proposals. Several key points were addressed, such as the European directive that makes the consumer liable for the first €150 of the fraud, alternatives to this system and practical issues related to fraud and current security measures available to eradicate it.

Web Page of the Project

PART 2

PAYMENT METHOD FRAUD IN THE EUROPEAN UNION

Consumer survey
Payment method fraud statistics

1. INTRODUCTION

In the face of massive expansion of non-cash methods of payment, numerous types of fraud have proliferated. The worsening economic situation has fanned the flames of fraud, with numerous attempts at fraud escalating through traditional means and the Internet.

Fraud does not occur in isolated cases, but is part of a complex network of organised gangs that seek to carry out indiscriminate swindles for low-value amounts in order to avoid being detected by the competent authorities.

It is imperative to emphasise that it is very difficult to obtain information on this type of fraud, as many are treated with the utmost confidentiality by the authorities and some cases never even see the light of day, as the victim often takes a long time to discover that he has been a victim of fraud.

Most of the statistics available are those published by various companies engaged in computer security; therefore, the data is confined to their clients' cases, thus limiting the quantitative representativeness, meaning that precautions must be taken when interpreting the data.

Aware of the current fraud problem, ADICAE is undertaking a European project relating to payment method fraud, supported by the European Commission. Among the materials for this project is this study, which we hope will be of interest and serve to inform you about the scale of fraud today

2. PAYMENT METHOD FRAUD IN THE EUROPEAN UNION

In the European Union, transnational fraud is more frequent than that which occurs within each country, especially in the case of distance payment transactions and, especially, through the Internet. According to European Commission data (COM (2004)), credit card fraud accounted for €600 million in 2000 - which equates to 0.07% of the turnover of this sector in this period with a greater increase in distance payments (through telephone, post and the Internet).

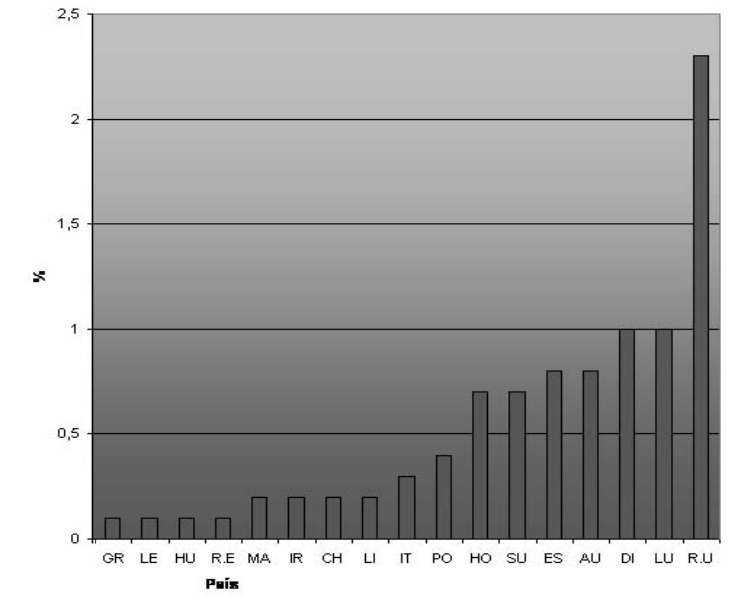
The most recent studies have shown that, in 2006, 500,000 businesses in the European Union were subjected to non-cash payment method fraud, with ten million fraudulent transactions, to the value of almost €1 billion, almost double the amount recorded in 2005. The countries particularly affected by fraud are the United Kingdom, France, Italy, Spain and Germany.

Below, we make use of the Ontsi report 2008, which is published on the Eurostat website, in order to explain this with figures.

In relation to fraud perpetrated with cards, the graph shows that the United Kingdom clearly stands out from other EU countries.

Of the individuals residing in the United Kingdom with access to Internet who have had a security problem, 2.3% have had a security problem with their cards. Luxembourg, Denmark and Spain also have quite a high percentage.

Card Frauds on the Internet



Proliferation of fraud can have a negative impact on consumer trust in payment systems and it is considered one of the main obstacles to the growth of electronic commerce. Other consequences of the spread of fraud are that it causes harm to the reputation of banks and it creates a false perception among consumers about the level of security in the use of payment instruments.

The spread and transnational nature of fraud makes the creation of a coherent prevention strategy at European level necessary, since, despite being effective, the steps already taken by Member States are not sufficient to counter the threat posed by payment fraud.

3. PAYMENT METHOD FRAUD IN SPAIN

According to the Spanish authorities, 46% of fraud in Spain in the last year are swindles, most of which were related to payment methods. The problem extends from swindles at ATMs to electronic theft, involving all methods of payment available to consumers.

3.1 ATM fraud

Spain has the largest number of ATMs per capita of any European country, with a network of approximately 61,000 machines. It is at these terminals that two different types of theft occur: physical and electronic.

According to Ministry of Interior annual figures, 450 robberies with violence or intimidation occur at ATMs.

Security problems experienced by users by autonomous region

A survey conducted by the multinational NCR, a specialist in electronic security for banks and financial institutions, found that, in Spain, one in every three users of ATMs considered that the security measures were insufficient.

This fear is understandable because, in addition to physical assaults, there are also electronic attacks, which are much more frequent and subtle, to the point that someone can be robbed without realising at the time.

3.2 The introduction of new technology in Spain and security problems

According to the annual report "Society of the Net 2007", published by ONTSI (National Observatory of Telecommunications and the Information Society), six out of ten people have accessed the Internet at some point. The regions that have the highest percentages of Internet users are Madrid, Catalonia and the Balearic Islands. With regard to frequency of access to the Net, 52.3% connected in the previous month, and 46.6% connected in the previous week.

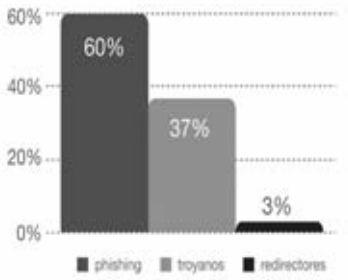
In terms of the most common security issues relating to computer use, 62.6% of Internet users received unwanted emails or spam and 49.1% of users had problems with computer viruses.

Receiving spam emails is most common in Catalonia, Cantabria and Madrid and Catalonia, and the Canary Islands and Aragon have the highest percentages of problems associated with computer viruses.

3.3 Internet fraud

Based on the "Online Fraud Report 2007" and the first half of 2008, published by the e-crime unit S21sec (A security company specialising in Internet fraud), we can extract the following figures on cyber fraud in Spain.

Online Fraud Report 2007, 2008



In the first six months of 2008, S21sec's e-crime unit detected a total of 1,842 cases of Internet fraud, targeting financial institutions in Spain, accounting for more than the total number of cases in 2007.

Phishing continues to be a major concern although it declines compared to previous years, 60% of fraud cases until June 2008, 66% in 2007, 85% in 2006. Attacks through the Internet have developed dramatically with more sophisticated techniques.

In the first half of 2008, the use of malicious code, programs that are surreptitiously downloaded to a user's computer while browsing the Internet, increased slightly with respect to 2007, accounting for 37% of cases compared to 31% detected in the previous year. Redirectors, a technique used to impede the closing of websites by dynamically redirecting to a phishing page, accounted for 3% of cases.

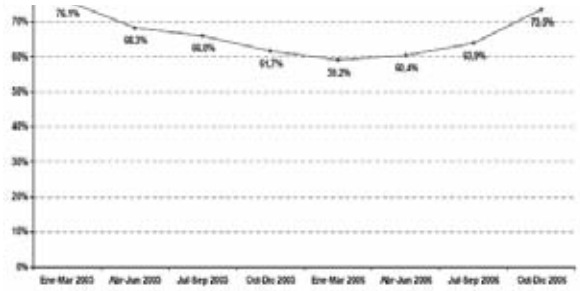
4. INTERNET FRAUD

4.1 An international perspective on Internet fraud

The scale of unwanted emails (spam)

Currently, almost three out of every four email messages (73.5%) are spam. Beyond the scale of spam, and the loss of resources that it can involve, it is necessary to analyse it as a potential criminal tool. Although only 4% of spam messages are directly recorded as fraudulent, it should be noted that messages that appear to be financial or commercial in nature could be a simple mask, which hides a second phase of the scam based on social engineering.

The international extent of spam in 2005 & 2006

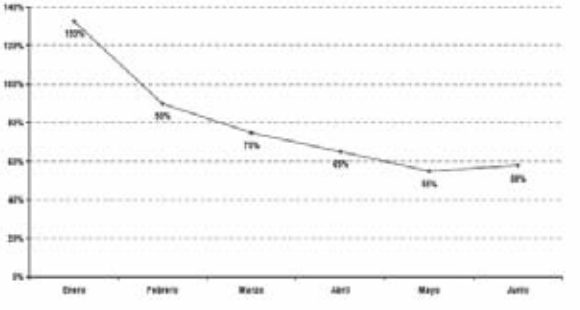


The relationship between spam and phishing

It would seem evident that this type of mass distribution messages could be an efficient way for criminals to attract victims.

The percentage of spam and phishing is quite low, but it should be borne in mind that they only cover a very specific type of fraud. As shown in the graph below, there is a downward trend in the percentage of phishing located in unsolicited emails.

Global evolution of the percentage of unwanted emails (spam), including online fraud attempts (phishing)



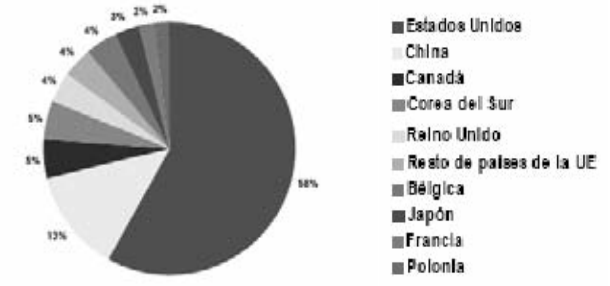
The origin of spam and phishing attacks

The origin of spam messages stands out. As shown in the graph below, the United States accounts for the highest number of emails sent, followed by a distant China. Both are countries with a large number of computers controlled remotely.

With regard to the origin of phishing attacks, the United States, South Korea and China account for more than 50% of servers that host phishing websites as shown in the following table.

The United States has the highest percentage of servers of this type, although decentralisation of these servers to other countries is confirmed, after a slight increase in 2005. (32% in 2004 to 24.7% in 2006).

Distribution of spam with respect to phishing according to geographic origin (%)



Classification of the top ten countries according to servers hosting phishing websites

Posición	Diciembre 2004	
1º	EEUU	32,0%
2º	China	12,0%
3º	Rep. Corea	11,0%
4º	Japón	2,8%
5º	Alemania	2,7%
6º	Francia	2,7%
7º	Brasil	2,7%
8º	Rumania	2,2%
9º	Canadá	2,1%
10º	India	2,1%
Posición	**Diciembre 2005**	
1º	EEUU	34,7%
2º	Rep. Corea	9,8%
3º	China	9,0%
4º	Alemania	3,8%
5º	Reino Unido	3,4%
6º	Japón	3,3%
7º	Taiwán	2,2%
8º	Rumania	2,0%
9º	Francia	2,0%
10º	Canadá	1.9%
Posición	**Diciembre 2006**	
1º	EEUU	24,7%
2º	Rep. Corea	15,7%
3º	China	14,2%
4º	Alemania	4,1%
5º	Canadá	3,1%
6º	Reino Unido	2,7%
7º	Francia	2,2%
8º	Japón	1,7%
9º	Rusia	1,7%
10º	Italia	1.7%

Phishing in figures

Between January 2005 and December 2006, the number of attacks doubled, exceeding 20,000 attacks per month at the end of last year. This trend means that in 2007, attacks will reach 250,000.

This growth can be explained by the development of tools designed to facilitate criminal activity and criminals' change in motivation.

Number of phishing attacks

Fraudulent websites

The number of fraudulent websites designed to carry out fraud increased by 100% in 2005. However, it was in 2006 when the number of fraudulent websites increased tenfold, which is explained by the sophistication of attacks and the use of other means of non-email communication to trick the user.

Number of fraudulent phishing websites

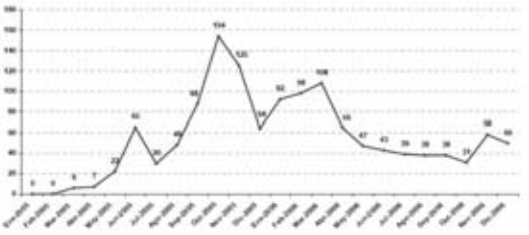
4.2 Overview of Internet fraud in Spain

The growth of phishing in Spain between 2005 and 2006 grew by more than 300%, from 293 attacks in 2005 to 1,184 in 2006.

Particularly significant was the increase of non-bank attacks, which reached levels of higher than 500%. This increase is driven largely by increased scam attacks (online fraudulent job offers), of which 344 cases were recorded in 2006.

The following graph shows how a significant increase occurred until October 2005, at which point, it begins to decline until the end of 2006.

Number of phishing attacks in Spain



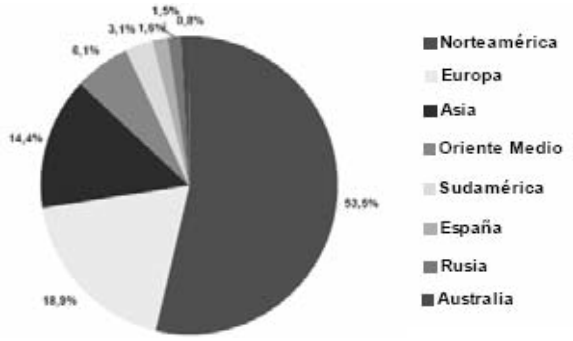
Regarding malicious code designed as a tool for phishing, Spain is situated in mid-high position in terms of the number of servers hosting these applications, although the trend is downward. Individually analysing data provided by the APWG regarding websites that host two specific types of malware (keyloggers and Trojans designed to carry out phishing), this trend is confirmed.

In 2006, there was a gradual decrease in the percentage of Spanish servers hosting keyloggers and Trojans up until May, at which point, there was an increase until June 2006, which saw a record global high of bank fraud attempts through the Internet.

The origin of phishing attacks in Spain

It should be borne in mind that not all attacks in Spain originate from within its borders. American servers are the source of over 50% of attacks. The statistics from the S21sec and VeriSign report further show that most of these attacks originate from abroad, as shown in the following graph (only 10 of the 609 cases analysed originated in Spain, less than 2%). Therefore, although it can be confirmed that Spain does not seem to be the best location as an operational base for cyber criminals, it does seem to be the target of attacks.

The origin of online fraudulent attacks in Spain (%)



4.3 The social impact of Internet fraud

Not only are there considerable monetary losses, but phishing also produces the negative effect of slowing down an economy that is increasingly becoming reliant on electronic transactions, due to lack of confidence in the security systems.

International reports, such as the study published by Entrust in 2005 (Securing Digital Identities & Information) provide highly revealing data about the financial sector, the most sensitive with respect to risk:

- 72% of Internet users who do not currently use online banking would do so if security were improved.
- 90% of current users of e-banking services would use new services if their identities were better protected.
- Security is an important issue for 65% of individuals when choosing which bank to use for online services.

5. A STUDY OF FRAUD IN NON-CASH PAYMENT METHODS

5.1 APPROACH

Analysis of the knowledgeability of Spanish people about fraud in non-cash payment methods, as well as the extent of fraud in society through a field study based on a survey.

It was conducted with all consumers who visited ADICAE at its various offices located throughout Spain, as well as carrying out surveys on the website and in the street. The analysis was carried out with the data collected.

Objectives

The objective was to achieve a global view that was significant in terms of the profile of non-cash payment method users. For this reason, different variables were included in the analysis relating to different aspects, which enabled the assessment of the following, among others:

- Consumer perception of security.
- Information provided to the user before making transactions.
- The degree of consumer satisfaction, as well as the main causes of complaints and claims.
- The introduction of new technology with special emphasis on the Internet and electronic banking.
- The most prevalent fraud in Spain.
- The fraud situation and extent in Spain.
- The structure of the field study

The survey was conducted nationally as we were seeking to extrapolate data from throughout the country.

To achieve this objective, surveys were conducted in several Spanish provinces. It is worth clarifying that the survey universe was the population resident in Spain so non-Spanish nationals were included.

The surveys were conducted by means of two different techniques:

1 Through the Internet with personal surveys sent by email.

2 Surveys done in person with ADICAE members, and others conducted in the street.

DETAILS

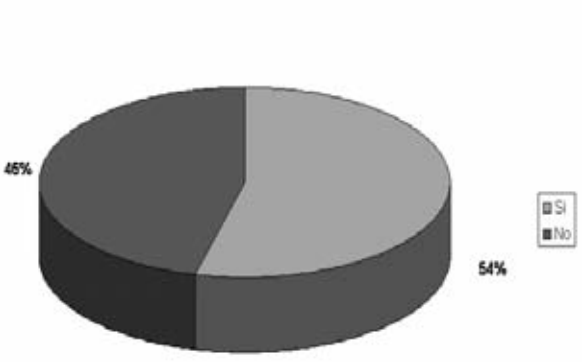
- Scope of the survey: National.
- Cities in which the survey was conducted: Zaragoza, Barcelona, Madrid, Seville, Castellón, Valencia, Valladolid, Cáceres and La Coruña.
- Survey universe: Population residing in Spain.
- Sample size: 1,200 respondents.
- Date of survey: From 1 January to 30 April 2009.

5.2 ANALYSIS OF THE RESULTS

5.2.1 NON-CASH PAYMENT METHOD PROBLEMS

The first important question to be asked was whether the respondent had experienced a technical problem with any method of payment. 53.76% answered yes, while 46.24% answered no.

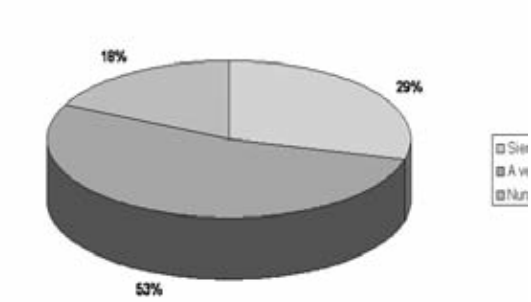
Problems with means of payment



5.2.2 SECURITY IN PAYMENT METHOD USE

Asked whether they felt secure when using any non-cash payment method, the respondents provided the following results. 29.27% said they always felt secure, 52.99% felt secure on some occasions and 17.74% did not feel safe at any time.

Do you feel secure when using a mean of payment?

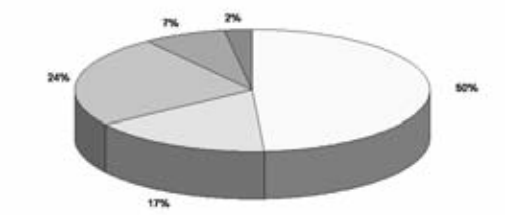


5.2.4 THE EMERGENCE OF THE INTERNET AND ONLINE SHOPPING IN SPAIN

Asked about how often they used the Internet, 13.91% said they never used it, 4.42% used it once a month, 11.26% once a week, 24.28% one hour per day and 46.14% more than one hour a day.

The next question asked related to the frequency of making online purchases on the Internet. 48.9% never made online purchases, 16,74% once a year, 24.45% between once and five times a year, 7.49% once a month and 2.42% more than once a month.

Problems with means of payment

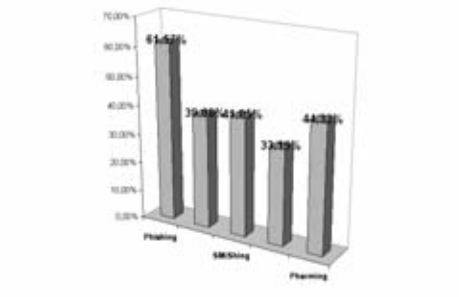


5.2.5 CONSUMER KNOWLEDGE OF THE DIFFERENT TYPES OF FRAUD

Respondents were asked about the most prevalent types of fraud today in order to find out which were the most well known.

Phishing was the most well known with 61.57% of respondents aware of it. 44.32% knew about Pharming, 41.05% were familiar with Smishing, 39.08% knew about Vishing and 33.19% were aware of the Scam.

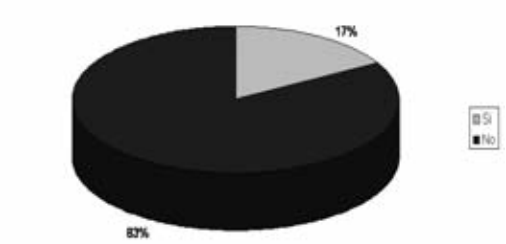
Have you ever heard about the following frauds?



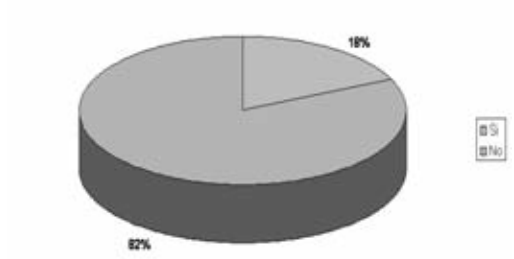
5.2.6 THE EXTENT OF PAYMENT METHOD FRAUD

In order to find out about the current extent of fraud, the respondents were asked whether they had ever suffered any payment method fraud. 16.7% answered yes and 83.3% said no. Of all respondents who had been a victim of fraud, 18.02% suffered some financial loss. Regarding the quantity of money lost, 17.65% had lost less than €50, 23.53% between €50 and €100, 31.37% between €100 and €500, and 27.45% more than €500.

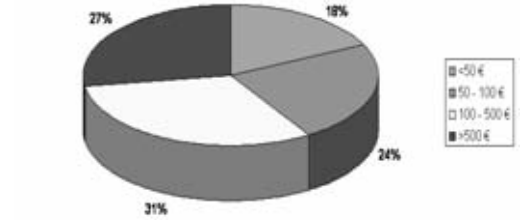
Have you ever been a victim in fraud of means of payment?



Did you suffer any economical damage?



Which amount was the fraud you suffered?



5.3 GENERAL CONCLUSIONS

After analysing the results, the conclusions are as follows:

Non-cash methods of payment are not technically efficient, since 53.76% of the population have had some technical problems when using them.

In this respect, we believe that it is necessary for banks, savings banks and payment method service providers to provide a good infrastructure (ATMs, POS, etc.), which would be well maintained.

Consumers are not usually informed about commissions charged for different methods of payment. 52.88% of the population say they are not informed about these costs. Furthermore, 59.69% of the population consider these commissions are too expensive.

Consumers feel insecure when using different methods of payment. 52.99% of the population sometimes feel insecure and 17.74% say they always feel insecure.

In terms of Internet penetration in Spain, we see that 46.14% of respondents browse the Internet more than one hour a day. However, this is not the case with online shopping, as 48.9% of the population never make purchases on the Internet.

The Spanish population's knowledge about different payment fraud is low. Only Phishing is familiar to more than half the population (61.57%); the other types of fraud remain largely unknown.

The problem of non-cash payment fraud is alarming. 16.7% of the population have been a victim of fraud.

Most financial losses are between €100 and €500 (31.37%), and it is also noteworthy that 27.45% of victims of fraud have suffered losses in excess of €500.

6. FRAUD COMPLAINTS MADE TO THE BANK OF SPAIN

From the statistical data obtained from reports by the Complaints Service of the Bank of Spain, relating to 2004 to 2007, and the quarterly reports relating to the four quarters of 2008, certain conclusions can be drawn in relation to this study:

1. The number of complaints has not experienced major variations, although each year has maintained an upward trend, with the exception of year 2005, in which the number of claims related to the fraudulent use of credit and debit cards decreased (albeit not significantly).

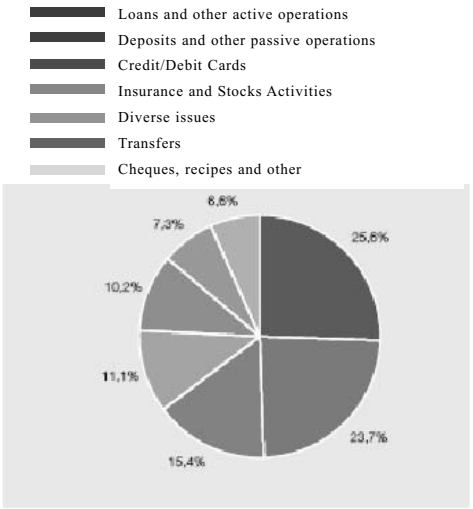
2. Claims relating to fraudulent transactions in electronic banking or Internet have risen, while for cheques and other methods, claims have decreased, which illustrates the need to bolster security systems as traditional payments decrease in favour of greater speed provided by the new electronic methods.

The numerous claims relating to non-cash payment methods is noticeable.

In 2007, for example, they accounted for 29.30%.

RESOLUTIONS BY THE NATIONAL BANK OF SPAIN

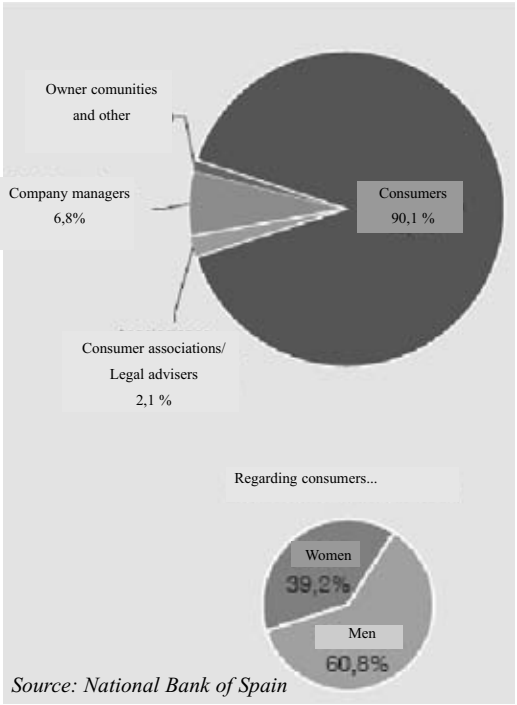
Areas



Source: National Bank of Spain

In 2007, the percentage of claims filed by consumers was 90.1%. That is to say, consumers continue to suffer abuse and bad practice, as they are less prepared than financial institutions.

TYPE OF CLAIMERS

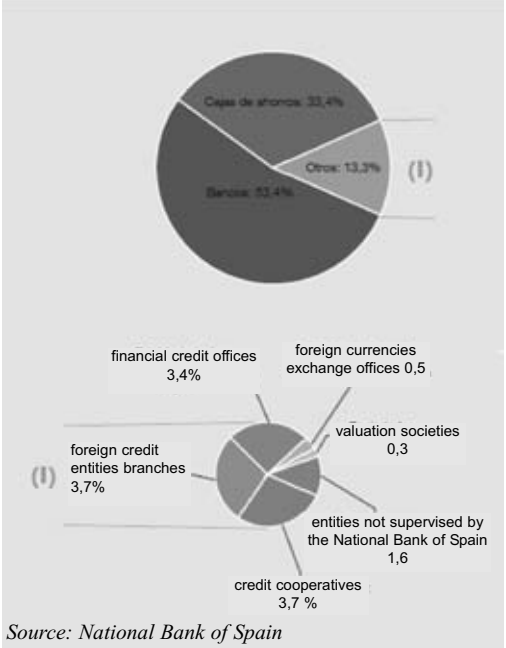


Source: National Bank of Spain

Over 50% of complaints are against banks, and approximately 30% are directed at savings banks.

This information shows that users of savings banks have a higher degree of satisfaction than banks

TYPES OF CLAIMANT



Source: National Bank of Spain

PART 3

Payment method users in the face of e-fr@ud

Events

Barcelona, may 2009

International Symposium

Payment method users

Place: **Hotel NH Rallye**
Travessera de les Corts, 150
Barcelona

Date: **11-12 May 2009**

PRESENTATION

Mr. Manuel Pardos Vicente

Chairman of ADICAE

Mr. Jordi Anguera i Camos

Director of the Catalonian Consumer Affairs Agency, Catalonia Regional Government

Mrs. Mª Dolores Fernández Gómez

Chairperson of the Department of Public Health and Consumer Affairs, Provincial Government of Barcelona

Mr. Josep Millán

Subdirector operativo de la Policía de la Generalitat, Mossos dÉscuadra

Mr. MANUEL PARDOS VICENTE

Chairman of ADICAE

Non-cash payment fraud has become a real headache for consumers and users since new payment and fund-transferring formulas were introduced. This is the first key point: since its beginnings, fraud has been ever present in the use and expansion of these payment methods. It has grown freely as its eradication was not a priority for operators, who were more concerned with growing than placing technical obstacles to stop criminal practices, which, ultimately, has proven to be one of the main reasons that users do not trust them.

This new phenomenon is moving at such a pace that many have already dubbed it e-fraud or cyber-crime. Today, consumers scarcely carry money around with them, only enough to get by. Even services that were traditionally paid for in cash, such as taxis, can now be paid by card. Cards are no longer a novelty. In Spain, there are more than 80 million of them, but fraud has yet to be eradicated in this area. These methods of payment have become so universal and permit the movement of such large amounts of money that criminals have found a real niche in their fraud. Perhaps it is because of the technical ease of committing fraud (copying the magnetic strip of a card, for example) or being encouraged by the severe lack of information for users in the management of such methods of payment, which ultimately leads to problems as the institutions rely on the carelessness or negligence of consumers to exonerate themselves from liability.

Through conducting a survey of users, ADICAE has been able to prove that fraud has affected 16% of consumers consulted. The average amount defrauded ranged from •100 to •500. These amounts, as well as being significant for consumers affected by the economic crisis, also provide two conclusions: firstly, that the proliferation of fraudulent behaviour has provided a huge profit for criminals, and, secondly, in many cases, criminal behaviour is qualified as theft, whose punishment is not a sufficient deterrent when the criminal is arrested.

For many years, through its publications and leaflets, ADICAE has been warning that the security of credit cards and other payment methods must be improved. The insertion of a chip instead of a magnetic strip has been very slow in Spain, as the institutions have called for a moratorium until the end of 2010. In the United Kingdom, the chip has succeeded in reducing card fraud by 60%. Spanish financial institutions, however, believe that the costs of incorporating the chip are greater than the benefits it produces. This is incorrect because it does not provide security and peace of mind to the customer. Moreover, in their calculations, institutions rely on the majority of case not being reported. Only when a claim is made well, through a consumer association or consumer institution, is the fraud considered to have actually occurred. While this situation remains unchanged, ADICAE believes that liability should fall on the issuing institution in 99% of cases, which leaves a small percentage for occasions when there is negligence by the customer (and it can be proved), who should also have been well informed about the use of the payment method. What is not acceptable is to assume negligence automatically. Institutions take advantage of users not knowing their rights.

In recent years, there has been greater awareness of the extent of the problem among operators, although not all have responded in a manner that one would expect. They should not wait for somebody else to do the work for them, since the point is that this requires the cooperation of users, government and the police. For this reason, ADICAE requested a project from the European Commission with many activities and impact, among which is this seminar, which brings together representatives from all sectors involved. It is through initiatives such as this that we hope that alternatives will emerge and there will be in depth discussions about the problem, which, if allowed to develop unchecked, may jeopardise the entire non-cash payment method network, which is being established at European level.

Mr. JORDI ANGUERA i CAMOS

Director of the Catalonian Consumer Affairs Agency, Catalonia Regional Government

Internet burst onto the scene a few years ago with such strength and today it has scarcely reached adolescence. Electronic commerce provides the possibility of purchasing products and services on a worldwide level, and opens up the possibility of improving and promoting competition. This approach is undoubtedly the best but it is important not to forget that two fundamental barriers could stand in the way:

1. Mistrust of payment methods, delivery problems, returns, the identity of the person behind the page.
2. Misuse of our details.

At the Catalonian Consumers Agency, we are unable to prosecute fraud because we are a government department, but it is undeniable that there exists criminal elements and, therefore, we do maintain permanent contact and coordination with the Police and prosecution authorities. From our point of view of administration and within our remit, we are clear that we must ensure that the information given to consumers is correct and that the terms and conditions that must appear in the contract conform to the rights of consumers.

In 2009, we have scheduled the inspection of services that are only offered online. The chosen areas are flights, travel, hotels and car rental. Surprisingly, in times of economic crisis, one of the few areas of business that increases is electronic commerce and that requires that consumer institutions ensure consumer rights. Our work focuses on prevention because conflict management alone is insufficient, therefore, we focus our efforts on providing information and instructing consumers, with courses that are tailored to the needs of Internet users. You could say we have adopted the maxim that if consumption changes, so must the consumer authorities.

Another initiative to create confidence relates to the fact that, since 2007, the Catalonian Consumer Affairs Agency can award the distinction of "Online confidence" to websites, so that users can identify those that comply with codes of good conduct, and whose content is verified by the authorities.

To sum up, in new times, it is necessary for the authorities, in partnership with consumer associations, to ensure security in electronic commerce and together eliminate or remove from the market those who wish to use this medium for unlawful purposes.

Mrs. Mª DOLORES GOMEZ FERNANDEZ

Chairperson of the Department of Public Health and Consumer Affairs, Provincial Government of Barcelona

For 20 years, the Provincial Government of Barcelona has been working to protect consumers. Our main focus of attention is the local councils, as they are the closest institutions to the citizens. For this reason, in 1982, the first municipal information offices (OMICs) were created in towns of over 50,000 inhabitants. In recent years, cases of fraud have increased among the population who are not familiar with these methods of payment. In this political reality, the Provincial Government of Barcelona gives technical, legal and financial support to local councils in the province, which are essential to develop an effective response.

During this time, we have helped to create over 25 OMICs and we offer technical assistance to over 270 municipalities. We directly manage enquiries and complaints from 230 municipalities that lack sufficient resources, in two ways: a) in person with six mobile units, and b) through electronic means.

We also work with local councils in implementing educational activities because we understand that information is a priority. We participate in advising council technicians and elected officials. Although the Provincial Government of Barcelona has no power to enforce control and market discipline, we carry out 4,000 visits to different municipalities per year.

This is a topical issue, but also complicated and difficult for the majority of citizens, which is why there is a lot of misinformation. I hope that the debate resulting from this project provides conclusions and I encourage consumers to put pressure on government to defend their rights even more effectively, if that is possible.

D. JOSEP MILLAN

Subdirector operativo de la Policía de la Generalitat, Mossos dÉscuadra

mossos d'esquadra

Desde los Mossos d'Esquadra tenemos claro que hay mucho trabajo por delante para garantizar los derechos de los usuarios. No basta con trabajar además de forma independiente, sino que se hace necesaria una labor coordinada de todos los agentes implicados ya que el fenómeno de internet y de pagos con medios distintos del efectivo estánen una fase de crecimiento exponencial como lo demuestran los siguientes datos:

- *94 % de las empresas catalanas tienen Internet*
- *54 % de los hogares catalanes tienen Internet*
- *Casi el 100% de los comercios tienen un TPV de cobro con tarjeta*

Si ha de crecer porque las nuevas necesidades del mercado así lo exigen, es necesario que se crezca con garantías, fortaleciendo tanto la seguridad jurídica como la tecnológica. A pesar de que tenemos un marco jurídico que permitiría proteger al "contratante débil" existe una notable inseguridad a la hora de pagar extendida entre los usuarios. En mi opinión la seguridad en las compras electrónicas depende de la forma en que las realizamos. En Internet hay que tomar una serie de medidas de precaución, igual que lo haríamos para cualquier otra transacción u operación realizada de forma cotidiana.

Sin embargo, cuando estos medios se ponen y siguen ocurriendo fraudes y estafas, se hace muy necesaria la implicación de las entidades emisoras, inversiones prácticas como las que se realizan en los chips, tener una política clara de seguridad así como tener personal formado y dar un servicio de calidad al cliente.

En este tipo de fraudes, las fuerzas de seguridad coincidimos en que los defraudadores van por delante de nosotros, incluso ya hay bandas que desarrollan algoritmos que proporcionaban el número de las tarjetas. ¿Qué hacemos desde la Policía? Los Mossos, tenemos un plan denominado "Internet segura" que se centra en la franja de edad entre los 8 y los 16 años, que representan aproximadamente 500.000 menores en Cataluña que se conectan a diario a la red. Es un plan dirigido a las escuelas, pero no solamente para los jóvenes sino también para los padres, para que en las Asociaciones de Padres de Alumnos se plantee el uso que hacen sus hijos de Internet. Como puede apreciarse la formación es clave para estas cuestiones, ya que tener que corregir deficiencias informativas y malas prácticas sobre la marcha resulta mucho más complejo.

CYBERCRIME UNDER INVESTIGATION BY EUROPEAN POLICE FORCES

OVERVIEW: E-FRAUD AS MASS CRIME

Lieutenant Osuna

Financial Crime Unit of the Civil Guard

Mr Antonio Mariscal

Head of Patrimony of the Criminal Investigation Department of the Catalonian Autonomous Police

Mr Antonio Donofrio

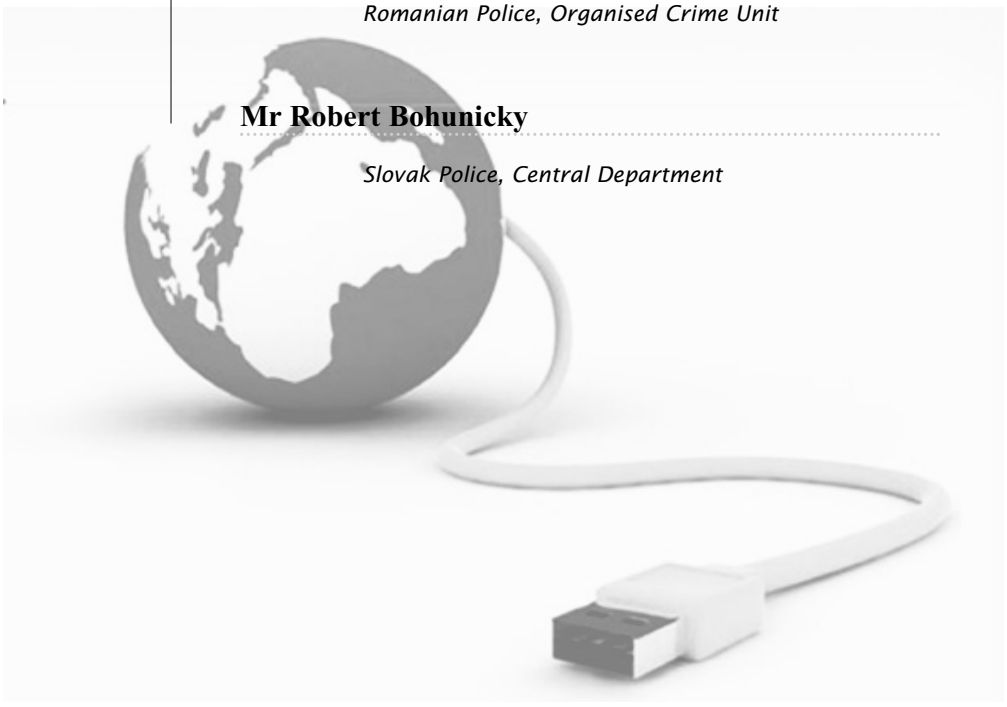
Head of Cybercrime, Finance Unit

Mr Marius Julián Joitia

Romanian Police, Organised Crime Unit

Mr Robert Bohunicky

Slovak Police, Central Department



CYBERCRIME UNDER INVESTIGATION BY EUROPEAN POLICE FORCES

Lieutenant Osuna

Financial Crime Unit of the Civil Guard

Law enforcement knows that when mass crime appears, it is necessary to work with as many people within the sector as possible. As these crimes also have a significant financial element, consumer associations, financial institutions, the judiciary, the prosecution authorities, etc, must find solutions. It is not just the responsibility of law enforcement.

What is fraud and how does it work? Tools to combat cybercrime.

By public prosecution or reported by citizens.

By order of the Public Prosecutor or judicial authority - in terms of criminal investigation: In this case, they assist the Public Prosecutor.

The main problems

Territoriality

Internet is not territorial. Anyone can commit an unlawful act in Spain from another country. Who is the competent authority in the matter?

- Where does the fraudulent activity take place?

- Where was the money withdrawn?

- Occasionally, they can be both.

The fact that this issue is not resolved from the beginning is a significant problem for the eradication of fraud.

Many types of violation: threats, disclosure of secrets

46%, the majority, are swindles and fraud. Counterfeiting cards, fraudulent e-commerce purchases, phishing, etc.

The law - problem with civil action

As soon as it has been decided that it is the jurisdiction of the courts of Spain and there are victims in other countries, our legislation requires that they be offered the possibility of a civil action. This results in problems for the process in terms of notifications, deadlines, etc.

Criminals defraud small amounts

Swindles are usually for amounts that are less than €400, so they are considered minor offences. It is therefore not possible to request or agree to searches of addresses, etc. Sometimes, cases are heard in lower courts in places where the victims reside, which reduces the financial significance of the crime.

When criminals use public networks or innocent people (mules) to distribute the defrauded funds

The so-called “mules” are innocent users who receive money from fraudulent transfers and

send it to eastern-European countries, as part of a job offer in which they are requested to carry out this transaction without being given further details.

Also problematic are cases in which criminals use unprotected public networks (wifi without passwords) to commit crimes as any investigation would affect the innocent users whose IP address has been used.

Critical assessment

The judicial authorities in Spain are not well prepared to take on and deal with the problem of fraud. Fortunately, notifications carried out by the judicial police are considered valid in the procedure. If it were necessary to do all of them, trials would be impossible.

There is an area that the authorities cannot reach and we must limit ourselves to prevention. What are the financial institutions doing to help in this prevention?

Mr Antonio Mariscal

Head of Patrimony of the Criminal Investigation Department of the Catalonian Autonomous Police

Prevention is the main weapon as the Internet and methods of payment are quite secure. They are not 100% secure, but if used wisely they reach that percentage. Certain groups are more vulnerable than others and with them further prevention is necessary.

The largest concern is that technically and organisationally simple swindles are significant, they generate large profits and therefore attract a greater number of criminals.

Moreover, if the fraud is detected, the criminal gets better with the police inquiries made and the offense is always one step ahead of the pursuer.

Fraud data

Groups are usually local.

In 2008, 3,700 crimes and other offences (handling, cloned cards, loss, theft).

Over 90% are thefts or losses.

No particular months stand out

Large cities account for the highest number of fraudulent transactions and those on the coast also experience high levels due to the number of foreign visitors.

Tips to prevent and manage fraud better:

- Be sensible and follow simple advice and guidelines. If fraud occurs judicial investigation and cooperation is complex.
- Special training for certain groups.
- The bank never requests your details. If in doubt, contact the bank.
- Ensure that the address in the browser begins with "https".
- In the bottom right-hand corner of the screen, there is a padlock and if clicked it is possible to see that who requested the certificate coincides with the bank with which we are operating.
- Do not respond to mass emails (not containing your name)
- Have good updated antivirus software and antispam filters.
- Phishing is no longer only associated with financial institutions, but also shopping centres.
- Make transactions in the morning as ATMs will have been checked.
- Be connected to the bank's system of notification of movements in order to detect suspicious transactions.
- Do not lose sight of the card or insert it in suspicious slots.
- Do not put receipts in litter bins
- Check components connected to your PC
- Destroy the hard drive of the PC when discarding it
- Do not use the same password for different accounts
- Do not use obvious information as passwords
- Disable Java and Javascript when browsing the Internet

Mr. Antonio Donofrio *Head of Cybercrime, Finance Unit*

The modus operandi of fraud, which is systematically repeated throughout Europe, is:

a) With the physical presence of card

Skimming: A small device that fits in the palm of hand. Data from the magnetic stripe of the credit card is obtained. With camera or cloning or duplicating the keypad.

Point of Sale fraud: The POS terminal is tampered with. The normal circuit of the device is interrupted and card and PIN data is sent to another computer. Then a card can be cloned.

b) Without the physical presence of the card

Phishing: Indiscriminate sending of emails to email accounts. If clicked, a page, which is similar to your bank's, will open and your details requested.

Keylogging: The can obtain screenshots of your computer screen and information relating to internet use, which are sent to the fraudster by email.

Trojans: Hidden in seemingly useful software.

Vishing: Derived from the combination of voice and phishing, using the telephone system by calling a number given in an SMS. The number is dialled and the visher can access the account.

Fraudsters also obtain information by searching though rubbish or stealing mail.

Detail of the Opening Panel during the speech of Mr. Manuel Pardos (at the center)

The phenomenon of the bank debits that are not returned

Bank debits that are not reimbursed because they are not detected within a month. The bank no longer reimburses. Million of euros per year. Hundreds of direct debits drawn. Only a small percentage exceeds €400 and it is not a crime.

Rip deal: Through the Internet but not with cards. The most serious threat. A simulated contract carried out over the Internet. People with properties for sale with high purchasing power. It is located in France. They claim to be a solvent business interested in investing in Spain. A deal is made in person. It is an excuse for laundering money. An average of €200,000. The money is brought by briefcase and the money is switched for counterfeit notes. They come to your house with possibly a false name.

THE STRATEGIC IMPORTANCE OF ROMANIA IN FRAUD

Mr Marius Julián Joitia *Romanian Police, Organised Crime Unit*

The Internet is not always secure. To improve this situation, prevention and combating cybercrime is necessary. After joining the EU, Romania has become a country that "exports" cyber criminals. Indeed, numerous Romanian criminal networks have been identified.

The law related to fraud in Romania distinguishes between a number of important concepts, among which is the definition of the payment method itself (transfer of funds and reimbursement of money).

The same law distinguishes between crimes, depending on the technique used:

- Counterfeiting
- Falsification of declarations
- Using a payment method without consent
- Accepting a payment, in full knowledge that it is irregular

Specific cases:

A phishing attack on a Romanian financial institution. Account holders were directed to a fake website that looked similar. APPLYING PHISHING TO ROMANIA.

NEW TECHNIQUES IN CREDIT CARD FRAUD

Mr Robert Bohunicky *Slovak Police, Central Department*

In 2005, the law changed with an article that included new fraud. Free movement complicates

the investigation of crime. There is usually more than one country involved.

In Slovakia, large quantities of money have been invested to improve the quality of life in the country. There is more tourism and this is attracting crime gangs as, so far, tourism is not well managed.

Payment card fraud

The most common is the theft of credit cards. It is easy for the offender and requires no particular skill.

ATM Skimming: An increase in cases and the number of criminal gangs involved.

POS terminals: Predominant throughout Europe. Risk is relatively low. It is difficult to detect.

There is a growing cooperation between banks and the police.

CHALLENGES FOR GOVERNMENT AND LEGISLATION IN THE FACE OF CONSUMER FRAUD IN ELECTRONIC COMMERCE

ELECTRONIC COMMERCE: WHO IS ON THE OTHER SIDE?

Mr Francesc Ruiz Toribio

Head of Inspection Services of the Catalonian Consumer Affairs Agency

THE NEED FOR SECURITY IN ELECTRONIC COMMERCE

Mrs María Arias Pou

Lecturer in Law and Computing at the European University of Madrid and lawyer specialising in electronic commerce

ELECTRONIC COMMERCE: WHO IS ON THE OTHER SIDE?

Mr. Francesc Ruiz Toribio

Head of Inspection Services of the Catalonian Consumer Affairs Agency

From the standpoint of government, the sale of products and services through the Internet has grown considerably in recent years.

Two main factors have increased the volume of business. One is the simplicity of the technique, which enables operation at a distance, it's fast, etc., and the other is the emergence of new companies or traditional companies that have incorporated this type of business. It is a new model of consumption that enables the comparison of prices, products, and therefore more competition. However, fraudsters, as well as the companies, are taking advantage of this situation.

The experience of consumer authorities

The work is mainly preventive with monitoring campaigns or also complaints from consumers who have been defrauded. The Catalonian Consumer Affairs Agency focuses on misleading advertising and unfair terms. An example of a sector that has experienced most growth is air transport, and the bad practice of pre-marking the voluntary insurance box when buying tickets has been pursued.

The boom in Internet business

Fourth quarter of 2008: €1.250 billion of business, not affected by the economic crisis. Transport, academies, etc.

Number of claims: Since 2005, a growth in the number of claims

Activities of the catalana´s asociation of consumer

The sale of tourism services on the Internet campaign: preventing incomplete information, misleading advertising and unfair terms.

Misleading advertising: Often, the price advertised is increased.

Eliminating methods such as open pricing, no fixed prices and "prices from" on the website, which do not actually exist.

Unfair terms: Those that stand out are terms that exclude or limit the liability of the company, eliminate consumer rights, allow modification of the terms and conditions in the provision of the service, are ambiguous or indeterminate, waive jurisdiction, and, in general, those that involve a lack of reciprocity in obligations.

Information: Consisting of verifying that information is provided through easy access and is also complete. Most consumer complaints predominantly relate to a lack of identification of the company providing the service.

THE NEED FOR SECURITY IN ELECTRONIC COMMERCE

Mrs María Arias Pou

Lecturer in Law and Computing at the European University of Madrid and lawyer specialising in electronic commerce

INTRODUCTION: THE NEED FOR SECURITY IN ELECTRONIC COMMERCE

One of the main obstacles to the development of electronic commerce is the **lack of confidence** among consumers and users, on the one hand, and service providers on the other.

This lack of confidence translates into the belief, not always correct, that the electronic environment does not provide the same security that exists in the "offline" environment.

The insecurity that is felt when performing electronic transactions, for example, on the Internet, is caused by various factors, including, among others:

- the lack of the physical presence of the parties,
- the need to enter card details to pay by electronic methods,
- the uncertainty of knowing whether the service provider advertising on the web page is on the other side of the screen or an impostor, and
- a long list of situations that prevent us or restrict us from taking advantage of the full benefits of the new technology put at our disposal.

1. DIRECT AND INDIRECT ELECTRONIC COMMERCE

When we talk about electronic commerce, it is with reference to commerce that is conducted by electronic methods. It is therefore not more than a new form of carrying out traditional business by using new information and communications technology that has been put within our reach.

It is not only limited to the Internet. Electronic commerce is an economic activity that is carried out by electronic means, to which all traditional rules of commerce apply, as well as the specific rules relating to that method.

Electronic commerce can be classified according to its purpose where a distinction can be made between direct and indirect electronic commerce. In the first, all commercial transactions are conducted by electronic means, while, in the second, offline methods have to be used to complete the transaction.

Insecurity and risks associated with e-commerce

In our view, there are various ways in which both legislators and service providers are promoting confidence in consumers and users of electronic commerce, specifically, electronic commerce on the Internet. In this regard, as stated by the legislature when explaining the rationale behind the electronic signature law: *"The development of the information society and the dissemination of positive effects derived from it, require widespread public confidence in electronic communications.*

However, recent information shows that there still exists mistrust on the part of the users of electronic transactions and, in general, communications that new technologies permit when transmitting information. This lack of confidence slows the development of the information society, in particular, government and electronic commerce." In addition to the electronic signature system, there are other ways to encourage confidence and credibility in electronic transactions, and they are:

- The right to prior information for the consumer. This right covers many issues and the most relevant are:
  - Article 10 of the LSSI (Information Society Services Law) relating to the general information that service providers must provide.
  - Article 27 of the LSSI concerning the duty to provide prior information in cases of electronic commerce.
  - Article 5 of the Organic Law on Data Protection, governing the collection of information for legal purposes.
- Security protocols that ensure the success of electronic methods of payment. Security protocols SSL and SET to which we refer later.
- Self-regulation codes of conduct, which, on a sectoral or company level, identify the obligations of service providers who commit to offering better services to consumers and users.
- Seals of quality that certify that the service provider satisfies the requirements of current legislation and corresponding codes of conduct.

2. "B2C" TRANSACTIONS IN ELECTRONIC COMMERCE: between company and consumer

B2C transactions are those that take place between Business and Consumer. For our purposes, we need to know, firstly, that the company, in terms of electronic commerce, is the service provider of the information society, as defined by the Annex to the LSSI, letter c, as a "natural or legal person who provides a service to the information society".

Secondly, the consumer or user who receives a service of the information society, according to letter d of the Annex of the aforementioned law, is a "natural or legal person who uses a service of the information society, whether or not for professional reasons". The adapted consumers' and users' text defines it in Article 3 as "natural or legal persons who operate in an area that is not business or professional".

2.1. The right to prior information in the LSSI

We emphasise the obligation of general information and the obligation of information prior and subsequent to electronic transactions.

-General information: Article 10 of the LSSI: Content and method of providing information.

This obligation, as we have noted, aims to provide consumers and Internet users with information that is necessary for situating them on the site in which they are browsing, and, moreover, provide them with information that is necessary to give them security or guarantees that they need to counter the distance and the absence of one of the parties in the relationship that is taking place. This obligation is contained in Article 10 of the LSSI, which was amended by Law 56/2007:

Access the following information by electronic means, in a permanent, easy, direct and free way:

a. identifying service provider information,
b. details of registry in the commercial register or other public register in which they were registered in order to acquire legal personality or only for the purposes of advertising,
c. price information of products or services,
d. whether they are subject to codes of conduct, and
e. two special cases related to service providers subject to prior authorisation and those engaged in a regulated profession.

The web page or site is therefore the place to facilitate information listed above.

This information should also be provided clearly and identifiably.

- Information prior to the electronic transaction: Article 27 of the LSSI.

The first obligation is to provide certain information to users, prior to the contract. This obligation is detailed in Article 27 of the LSSI and was amended by LISI (Information Society Promotion Law), including new reference to the fact that this prior information should be provided in accordance with the method of contracting.

Content of the prior information

The user must be offered information that refers to:
a. the procedures necessary to conclude the transaction
b. whether the electronic document in which the contract is formalised will be filed and whether this will be accessible,
c. technical means that are put at the disposal of the user to identify and correct errors when inputting details, and
d. the language or languages in which the contract may be formalised.

This information must not be provided in the event that the contract was carried out through an exchange of emails exclusively or other equivalent communication.

The information requested prior to electronic contracting must be provided clearly, understandably and unambiguously to the user. If contracts include CGC, they must comply with rules governing the incorporation of these clauses in a contract.

- Information subsequent to contract

The second specific obligation that services providers have is the obligation of information after the contract. Regulated by Article 28 of the LSSI, this obligation consists of the provider being obliged to confirm receipt of the acceptance.La LSSI describe **dos formas de cumplimiento**, por parte del prestador de servicios, de la obligación de la información posterior:

The LSSI describes two forms of compliance by the service provider:
- The first refers to the sending of an acknowledgment by email, or other method of equivalent electronic communication to the address the consumer has indicated, within twenty-four hours of receipt of acceptance. This form of compliance involves written confirmation that acceptance of the offer has been received and the delivery period begins to run for the goods or service.
- The second form of compliance involves confirmation of acceptance, by any means equivalent to that used in the transaction procedure, as soon as the consumer has completed this procedure, provided that confirmation can be filed by the recipient.

The LSSI also stipulates that the recipient must comply with the obligation of confirming and in this case require the provider to facilitate compliance with this obligation.

Documentary confirmation

With respect to documentary confirmation of electronic contracting, we must mention Royal Decree 1906/1999 relating to electronic contracts that incorporate terms and conditions of contracting, which in Article 3 addresses this issue by establishing the obligation of sending the user an acknowledgement, not of receipt of acceptance, but of the documentation that contains all contract terms.

That is, when electronic contracting is carried out, the user must be provided with all contractual terms that constitute the contract documentation, in which all points are described immediately or, at the latest, at the time of delivery of the product or the commencement of the contract.

The moment of completing the electronic contract

In the electronic signature, the time and date of acceptance are verified and the problem will not arise to clarify this point but the fundamental problem is none other than the conflicting interests of the contracting parties. The buyer wants his acceptance to produce results as soon as possible, when posting the letter, the theory of issuance, collection, until the passing of the LSSI, by our Commercial Code, while the seller wants to wait to receive the letter accepting his offer of goods or services, the theory of reception, collection until the same date by the Civil Code.

In the electronic environment the same occurs, therefore, the LSSI establishes a presumption that it is understood that acceptance of the offer has been received and confirmation when the parties have a record of it.

Thus, Article 28 of the LSSI concludes in its second paragraph: "In the event of receipt of the

acceptance being confirmed by an acknowledgment of receipt, it is presumed that the recipient may have the referred documentary evidence, since it has been stored in the server in which the email account is registered, or in the device used for receiving communications."

3. ELECTRONIC PAYMENT FRAUD

With reference to security in electronic commerce, it is necessary to make reference to one of the issues that causes most reluctance among consumers and users in accepting electronic commerce, and, in particular electronic commerce through the Internet: payment through electronic means.

In this type of contracting, the consideration of the consumer or recipient will be, in most cases, payment of money or a sign that represents it. The speed, convenience and facilities provided by contracting by electronic means must not, in our opinion, become paralysed and be unable to advance because we do not have safe and reliable methods of payment that we are invited to contract using these methods.

That said, we will analyse electronic payments, for if we remember that contracting through electronic means is firstly contracting and then electronic means, which means that the study of payment by electronic methods leads us to firstly consider what the payment is and what regulation exists in our judicial system, in order to then analyse the more specific aspects of the electronic environment.

Special reference to payment by card

There are many different electronic payment instruments, but we will focus on cards as

methods of electronic payment.

We can begin by saying that payment cards are the best-known electronic payment instrument and most widely used in society and long before the emergence of the Internet. Notwithstanding that, it may be regarded as one of the electronic methods of payment that is most used on the Internet, since its beginnings and it is still being used today. Payment cards can be of different types depending on various criteria, such as, the moment in which payment is made or the use or uses that it can provide more or less limited. We can therefore distinguish between credit cards, which defer payment until an agreed date, debit cards, in which payment is made automatically or almost automatically and store cards, which are issued by shops for payments made in the acquisition of

There were about one hundred attendants, who where representatives of stakeholders

goods or services offered by them and that provide several advantages to account holders, such as postponing payment without interest until a certain date or certain advantages in the financing of goods or services

that are acquired in their shops.

Payment cards are documents that result from contracts between cardholders and issuing banks, in which all terms and conditions of use of the cards are included. In addition to the relationship between these two, there is also a third relationship with those establishments that accept cards as payment for the acquisition of goods or services that they provide.

And in relation to methods of payment, they account for the majority of buyers, 54% prefer to pay for their online purchases with a credit or debit card. This has been maintained throughout recent years, although, in 2007, preference among buyers was not as evident as in previous years, with other forms of payment gaining ground. In this way, and without showing very positive development, forms of payment such as cash (27.7%), bank transfers (11.7%) or even

PayPal (4.5%) are considered favourites by a higher percentage of buyers than in 2006.

The youngest (24 and under) and residents in small municipalities (fewer than 10,000 inhabitants) prefer cash more than most buyers, while those over 50 years, university students and individuals with a medium to high socioeconomic level mostly opt for credit cards. Other payment methods such as PayPal are more popular among the youngest (under 25s) and Internet users in larger cities (over 100,000 inhabitants).

Security Protocols

The methods that provide safe routes through which payments are made on the Internet are security protocols. These protocols offer security and provide the confidence that consumers and users need in their electronic transactions. There are two main protocols, Secure Socket Layer (SSL) and Secure Electronic Transactions (SET). Both are used for credit or debit card payment through the Internet.

The SSL protocol was developed by Netscape to enable encrypted and secure transmission over the Internet. At present, it is used most for transmitting data and, at the same time, to carry out electronic payment transactions.

The SSL protocol is a secure data transmission protocol used, among other functions, for payment by electronic means, in which the data that is transmitted relates to payment cards. But, unlike the SET protocol, it is not specially designed to guarantee security in electronic transaction payments.

4. CODES OF CONDUCT AND SEALS OF QUALITY

Codes of conduct are systems of self-regulation based on the commitment of offering consumers and users, in a particular sector, protection, guarantees, and security, which exceeds that which is provided by law. It is materially impossible for legislators to regulate all sectors that have weak elements that need to be protected and therefore self-regulatory systems are encouraged.

The Ministry of Industry, Tourism and Trade, through its website www.lssi.es states that "the Internet is an ideal environment for the development of self-regulation given that it is dynamic and constantly evolving, and requires flexible regulation, where private initiative has great strength and there is also a particular awareness of the desirability of having adequate performance models that improve the confidence of service users ".

An example of a code of conduct is "the Online Trust Code", which, in respect to payment method security in Article 21, establishes:

1. Service providers must provide consumers with simple and secure payment mechanisms, and ensure that they are completely up-to-date on all developments in the field.

2. Service providers must adopt appropriate security systems that are trustworthy to safeguard the security, integrity and confidentiality of financial transactions and payments made by consumers, who must be informed as clearly and simply as possible about the level of protection that applies and the use of secure connections (such as SSL or others), before providing financial information.

The guarantee offered by these codes of conduct is that of prior control as stated in Article 35 of the Code:

Institutions that apply for membership of this system of self-regulation must undergo pre-verification of compliance with the rules that apply to them in this Code of Ethics relating to their websites to obtain the Online Trust Seal".

As is clear from the above, intrinsically linked to codes of conduct are marks or seals of quality, whose incorporation in such a code requires fulfilment of additional guarantees to those provided by the regulations governing the sector in question.

The granting of a seal of quality associated with certain products or services is based on the power of such symbols, logos or labels to inspire confidence in consumers and users, so that they place their trust in a provider that holds the seal and not in another because of the guarantees associated with it.

Paragraph 3 of the rationale behind the LFE defines the quality seals and states: "they are effective means of convincing users of the advantages of products and services of electronic certification, and it is necessary to make these external symbols easily available for those who offer them to the public".

5. CONCLUSIONS

1. Requirements for the Internet as a commercial outlet

It has been shown that consumers attach great importance to being provided with clear information on their rights (78%), or sales contracts (72.6%) or even goods to be bought and costs generated by the purchase (75%).

Another key aspect is the availability of information relating to security elements that companies provide regarding security mechanisms (76.4%) or that it is fully identified (77.3%). Also essential is the payment method. Buyers consider it important that companies offer their preferred method of payment (72.7%). In this regard, the majority of buyers (54%) prefer to pay online by credit or debit card (mainly credit card).

2. Satisfaction with online shopping

Payment problems (payment fraud, final price different to that agreed, or problems with the payment itself), in spite of being those that most discourage non-buyers, are not significant. Only 10.8% said that they had experienced difficulties in this area, compared to 42.7% who had reported logistical problems or 49.3% who complained of non-logistical problems.

Despite the low incidence of problems with payment processes, the survey reflects an improvement in this regard or in buyers' perceptions of the security of financial data, as a key element for buyers to increase Internet purchases.

3. Assessment of quality seals

Buyers' perceptions are very positive regarding these seals, with six out of ten (59.9%) stating that they had taken this into account when making online purchases.

4. Obstacles to electronic commerce

Internet users who made no purchases in 2007 stated their preference for making purchases in shops so that they could see what they were buying (38.3%).

However, mistrust of the Internet in relation to personal or banking information remains significant.

25.7% of those who do not buy on the Internet stated that they did not believe it to be a secure method and 22% specifically cited mistrust of payment methods and 14% indicated that the Internet concerned them in relation to supplying their personal information.

THE VOICE OF THE CONSUMER: QUESTIONS AND REFLECTIONS

The importance of information. Informed user but what to do with unfair terms in adhesion contracts. This is emphasised in electronic commerce where there is less immediacy. The authorities impose penalties, but only in civil proceedings and for specific cases that do not help the consumer.

A serious lack of European harmonisation in the regulations: Different customs: In France, hotels, before requesting documentation, ask for your credit card. If you do not use the services of the hotel, you are charged a fee. The French custom is to charge for the first night just for entering.

Self-regulation and soft law: €150. Up-to-date and complete regulation is required. Self-regulation is necessary because it involves a step forward for companies and it cannot be contrary to law. Also, seals of quality are granted for those that deserve them.

Electronic commerce law has undergone many modifications to update it and provide concrete solutions. 7 out of 10 consumers argue that the lack of information creates most uncertainty and for this reason, electronic commerce law focuses on this problem. But, there can be loopholes that cannot be overcome by self-regulation alone. It is necessary to harmonise. On 1 November 2009, Member States must adapt to the single payment method market. The majority are not prepared.

LIABILITY IN THE FACE OF FRAUD IS THE CONSUMER ALWAYS LIABLE?

NEW TECHNOLOGIES AND ISSUES ON CONSUMER COMPLAINTS

Mr. Jose Antonio Somalo Giménez

Customer Ombudsman for Catalonian Savings Banks

EXCESSIVE OBLIGATIONS AND LIABILITY FOR USERS DAVID CASELLAS

Mr. David Casellas

Lawyer at ADICAE

FRAUD AND USER LIABILITY IN LITHUANIA

Mr. Gediminas Buciunas

Prosecutor and University Lecturer in Lithuania (Specialising in Evidence and Forensic Law)

LIABILITY IN THE FACE OF FRAUD IS THE CONSUMER ALWAYS LIABLE?

Mr. Jose Antonio Somalo Giménez

Customer Ombudsman for Catalonian Savings Banks

Introduction

Systems are standardised in Europe, almost 100% of transactions are made with Visa or Mastercard. Spain, at the end of 2008, was 96% standardised.

With regard to fraud, the biggest problem is the cloning of cards; a problem that would be resolved by the insertion of a chip, which is yet to become a reality in all banks. Standardisation has the theoretical advantage that the burden of proof has been invested

in favour of the consumer, although this has to be put into practice by all banks for it not to remain as an unrealised benefit. The recording of PINs with cameras is used abroad, which complicates the pursuit of fraud. This should not be a problem for the user, as the bank will assume responsibility under the new liability system that is being proposed.

Another method that has been created to assist in the eradication of the harmful effects of fraud is insurance against being defrauded with a liability limit, which means that, if the user gives notification within a certain period of time (24 - 48 hours), he is protected.

Transparency is important in this type of insurance so that the consumer knows what is covered and what is excluded. Should fraud occur, both parties are clear in terms of their liability.

The effects of the economic crisis in customer claims against banks:

2005 was a turning point as there was a loss of credit from cards, which led to fees increasing and an attempt to incentivise use (purchases by instalments - consumer credit).

EXCESSIVE OBLIGATIONS AND LIABILITY FOR USERS

Mr. David Casellas

Lawyer at ADICAE

Card payment in distance purchases has always generated certain mistrust. The fact that the consumer has to give his card number over the Internet causes misgivings about the possibility of third parties gaining access to such information, which could be used to carry out fraudulent acts, even without being identified. The physical absence of the parties prevents identification of both the cardholder and the card itself, meaning that it is not known who is using it for the transaction. Moreover, a signed receipt by the cardholder is not obtained.

In practice, the company only requests the card number and expiry date. Currently, it is quite common to request that the PIN be typed in to execute the payment order, which can largely guarantee the security of the transaction.

To avoid adverse consequences for the cardholder in electronic commerce caused by unauthorised parties, the technique offers us various security measures and protocols to prevent such abuse, even though they do not offer total security. In the event that this security "ex ante" does not produce the desired effect, legislation protects the cardholder "ex post" against misuse or fraud.

In criminal law, Article 248.2 of the Penal Code classifies the crime of fraud, and considers "guilty of fraud, those, who for motives of profit and by computer manipulation or similar device, succeed in the transfer, without consent, of any assets to the detriment of a third party. This is particularly designed, among others things, for the cloning of cards.

It is therefore necessary that knowledge of the card number results from computer manipulation or other similar device.

In the civil law, Article 106 of the Revised General Law for the Protection of Consumers and Users regulates card payments. This article states the following:

a) Firstly, the cardholder, whose number has been improperly or fraudulently used by a third party, has the right to cancel the charge made by the credit institution, which is obliged, within a period not exceeding thirty days from the communication of the request for cancellation, to adjust the respective debit and reimbursement entries of the purchaser's and company's accounts, without the bank being able to determine, at that moment, if card payment for this distance sale had been carried out or not by a third party. This solution is also achieved by application of the terms agreed to in the electronic commerce contract.

b) Secondly, once the accounting adjustments have been carried out in the respective accounts of the consumer and the cardholder and the company from which the goods or services were purchased on the Internet, it is the company that has to prove that the card number used to pay for the purchases was entered by the legitimate cardholder and, in this case, demand compensation for damages caused as a result of the improper cancellation of the charge, together with the cancellation of this transaction or compliance with what was agreed, according to the agreement.

c) Thirdly, the bank that issues the card is only liable for misuse or fraudulent use of the card number if it fails to comply with the issuing contract signed with the cardholder: for example, for having provided the cardholder's personal and non-transferable details to a third party.

d) Finally, negligence on the part of the cardholder makes him liable before the company and issuing bank, for damages caused (for example, by communicating to a third party the card number or failure to notify the issuing bank of the loss or theft of the card), the burden of proof being with the cardholder.

Practical obligations for issuer, bank and consumer

The cardholder, from the time the bank informs of the existence of one or more charges relating to the account associated with the card, may request the immediate cancellation of those that he believes have been fraudulently or improperly carried out by a third party.

When such a request for cancellation is made, the company bears the cost of the transaction, without being able to check if, indeed, the card number has been properly used by the cardholder or improperly or fraudulently by a third party. The cardholder therefore receives prompt and effective protection.

The bank must, without delay, complete the rele-

vant entries in the respective accounts of the cardholder and the company. Similar to the provisions of Article 104 of the Revised General Law for the Protection of Consumers and Users, this period should not exceed thirty days. In the case referred to in Article 106.1 of the same law, the distance sale has not been completed, since the cardholder has not agreed with the company's offer. In this case, it is an authorised third party who enters the card number. The issuing bank sends the cardholder the PIN, which adds greater security in purchasing goods and services online.

In electronic sales, entering the PIN implies identification of the owner, which is necessary for the electronic payment system to function properly. With the PIN, the bank accepts the sale if the cardholder has funds. However, the PIN can be used improperly or fraudulently by a third party. In this case, the PIN does not provide complete security for card payments in electronic sales, because anyone who knows the code can use the Internet to purchase goods and services. Logically, the payment card is a personal proof of identity and is non-transferable, so correct use of the card represents respect for the confidentiality of the PIN. Non-compliance with this charge implies the cardholder's non-compliance.

However, even in the event of negligence on the part of the cardholder by communicating the PIN to a third party or not having notified the bank of the loss or theft of the card, it is still possible to cancel the charge, although later the company and the card issuer can claim for damages caused by his conduct.

In Spain, there is no positive legislation relating to credit cards or even fiscal or administrative provisions.

In terms of the parties involved in legal considerations, one of the main problems with compliance is the case of theft or loss, as the agreed conditions establish the obligation of the cardholder to notify the issuer within certain time frames, by telephone, in writing in a maximum of three days, etc.

The cardholder is considered liable for fraudulent use of the card by a third party if the conditions are not met. The cardholder can maintain that he was unaware of the loss or theft up until the charge is presented.

Case study

A case was resolved in a court ruling in April 2006, issued by the Provincial Court of the Balearic Islands.

A cardholder requested that the Bank reimburse his account for a charge he did not recognise, made by a credit card issued by the bank but which the cardholder denied receiving. The bank denied the reimbursement on the grounds that it had sent the card, but could not prove it. The cardholder was subsequently obliged to sue the bank, and the ruling determined the bank's liability because "even assuming that the card was sent to the address of the plaintiff, which was not recorded other than as manifested by the defendant, this is not sufficient to prove that it was received and subsequently used, in this regard, it could have been acquired by a third party". In this case, the bank could not certify to whom or when delivery of the card was made, as it could not provide a receipt certifying that delivery was made to the account holder. In the absence of such key evidence from the defendant, liability must be attributed to the bank, which had the duty of care for the amounts deposited by the plaintiff, and no right to authorise withdrawals that were not authorised by the plaintiff's signature.

That is to say, as the bank was unable to certify the delivery of the card to the account holder, any fraudulent use of the card results in the bank being liable as its obligation was to ensure that only the legitimate holder of the account could have access to the funds. Any exemption of liability for the bank, when an irregular or improper withdrawal has been made, must be based on proof that it had used all means at its disposal for the proper functioning of the concatenated mechanism of funds-ATM-credit card-account holder, and that proof is incumbent upon the bank as the creator of such a mechanism and because the initial acts of the proper functioning were acts that it must carry out.

This breach of contract is not derived from electronic distance purchases, but a separate contract, such as the issuing of a payment card, which did not involve the company that provided the goods or services to third parties who illegally used the payment card. However, if the illegal payment was made after the card number was made known as a result of the loss or theft of the card, and the cardholder had not reported it to the bank, this negligence would make him liable for damage caused. Nevertheless, in this case, the cancellation of the charge would initially have to be borne by the company, which would then claim the cardholder's liability.

In this case, a clause is usually agreed in card issuing contracts that limits the liability of the card holder up to a certain amount for loss or theft of the card until the moment that notification of the circumstances is given to the bank.

In summary and in relation to fraudulent use of credit cards, we can establish a series of obligations for the cardholder (the consumer), the card issuer (the bank or savings bank), and the company, as well as various recommendations that the AICEC-ADICAE Association passes on to its partners and users of financial services in general:

Cardholder obligations:

- Use the card correctly, and be especially diligent with the PIN.

What must we not do?

- Write down the PIN on the card or accompanying documents
- Use easily identifiable information as the PIN, such as date of birth.
- Leave the card in visible places, for example, the seat of a car.
- Throw away receipts and invoices for purchases before the account is charged.
- Immediately report loss or theft to the issuer.

What happens in the event of a forged signature?

The problem that arises here is who is liable in the event of an invoice with a forged signature. According to the EC Recommendation of 17 November 1988, up until the notification, the cardholder's liability is limited to €150. This recommendation, while not binding, has been adopted by the vast majority of credit institutions in Spain. It is customary that the credit card contract considers that, before notification, the cardholder is liable for a certain amount, except in the

This brings us to real case, in which the cardholder took 24 days to report the theft of a card, which was when the statement arrived. Total payments amounted to €2,500.

Who was liable for those charges?

The bank argued that:

a) the customer had a duty to prevent the theft as he was responsible for the safekeeping of the card, and

b) the €150 limitation of cardholder liability in the contract is only valid when the loss or theft is reported within 24 hours.

Firstly, regarding the duty to prevent theft of the card, the Provincial Court of Madrid that ruled on this case did not consider that the cardholder had acted imprudently as the duty of care (Article 1104 of the Civil Code) cannot, in this case, consist of an obligation to constantly verify possession of the card.

As was argued, correct use of the card does not solely depend on custody but the verification and communication system of the payment system as well as the obligation of companies to check the identity of the card user.

Secondly, the reporting of the theft, according to the court, is just one form of caution among others, and not sufficient to justify the bank's exemption from liability.

Furthermore, the ruling did not consider the cardholder negligent as he reported the theft when he received the statement.

But, by contrast, it showed that the bank had failed to respect the daily limit of €310 agreed with the cardholder and the establishments failed in their duty to verify user identity of the card.

Moreover, the Court stated that, since cards are a source of profit for banks, they have a duty to address the serious consequences arising from their unlawful use.

event that he acted fraudulently or with gross negligence. In any case, after the notification, the bank is liable.

Promptly notify the issuer of any unauthorised transactions or any other error or irregularity in the management of the account on the part of the issuer.

We must bear in mind the following:

- In the event of a dispute with the cardholder, the issuer has to prove that the transaction was properly recorded.
- The proof lies with the issuer because it has the responsibility to keep a record of operations performed.
- The issuer is liable for the losses caused by malfunction of the system under its control.

The card issuer's obligations.

- To issue the card and make it available to the cardholder. Two aspects must be taken into account:
- It is prohibited to send cards that have not been requested, but use in considered acceptance.
- The card must be delivered to the cardholder in such a way that ensures receipt.
- To respect the limit that has been established in the contract.
- The invoices that the cardholder signs with the establishments must be paid. Responsibility must not be taken when there has been fraud on the part of the cardholder or the establishment.
- The cardholder should periodically receive a detailed statement of transactions.
- There must be a record of transactions.
- Technical support must be provided to establishments in order that credit card transactions can be made.

Obligations of participating establishments

- To accept cards as payment.
- They must verify that the person using the card is the cardholder and it is used correctly.

FRAUD AND USER LIABILITY IN LITHUANIA

Mr. Gediminas Buciunas

Prosecutor and University Lecturer in Lithuania (Specialising in Evidence and Forensic Law)

The fraud situation in Lithuania

In Lithuania, there are 4 million banks cards, and only 3 million inhabitants.

Firstly, it is important to unify the legal terminology as a starting point.

Losses can be criminal or not criminal

Criminal liability:

Article 214 of the Penal Code provides for the falsification of electronic methods of payment or illegal possession of an electronic payment method.

Civil liability:

In Lithuanian law, the bank compensates for losses when the cardholder loses the credit card, but not completely as liability is usually limited in the contract.

In Lithuania, there are two consumer laws:

The Consumers Protection Law.

Payments Law (Article 21).

Wilful intent or blatant negligence:

The option is related to consumer rights. When the Bank does not want to deal with losses it alleges that negligence was reckless.

The liability limit of €150 is not applied in these cases. If a card is stolen and the theft is reported, the bank will only compensate €150.

But according to Lithuanian law, the minimum wage per hour is €1.40 and the minimum salary is €232 per month. This limit of €150 Euros is extremely outdated as, in Western Europe, salaries are six times higher. In Lithuania, based on a specific case, it was found that a person was able to go to six supermarkets and use a stolen card with complete freedom.

Measures taken by the Lithuanian authorities:

Improvement of the police force in Lithuanian.

Informal education especially for the elderly.

Films broadcast on television by the Lithuanian National Consumers Federation.

THE VOICE OF THE CONSUMER: QUESTIONS AND REFLECTIONS

Question - The Catalonian savings bank ombudsman mentioned the real possibility of users making a claim to the courts and using consumer arbitration and my question is whether Catalonian savings banks are attached to consumer arbitration because the statement surprised me.

Answer - I was not referring to consumer arbitration, but arbitration in general because there are many types; in general, arbitration cannot work without the consent of both parties. If one party does not consent, there is no arbitration, other avenues are taken, as happens in most cases.

Question - I would also like to know if other countries, which are present today, have implemented consumer arbitration as in Spain.

Answer - The arbitration system only exists in Spain and Portugal. In other European countries, there are extrajudicial systems of conflict resolution, although financial services are excluded.

Question – It was mentioned that it is prohibited to send cards that have not been requested and I was wondering why teenagers with bank accounts, who reach eighteen years of age, are sent cards without applying for them.

Answer - The reality is that a lot of publicity is sent. It is true that warnings about the correct use of cards are given, in some cases more clearly than others, but the point is that any unrequested service requires specific protection and, moreover, if the credit card is sent to a minor, security should be even greater. The card should not be sent.

Answer 2 - The criterion of the Catalonian savings bank ombudsman, in these cases, is that, whenever the card is unsolicited, the customer receives a favourable decision, because clearly the card was not requested and no consent was given.

Question – The ombudsman cannot comment on the terms of the contract, but we have seen that in terms of cards and electronic banking, there are clauses that limit consumer liability and there have been court rulings that have declared this issue proved. Although the ombudsman cannot cancel or amend contracts, at least, pay some attention to Catalonian savings bank so that they improve these terms?

Answer - Jose Antonio Somalo - I would like to say that we have regular meetings, and we highlight everything that seems unfair. The proof is that contracts are being changed; there are many clauses that in effect are poorly written, but we cannot get more because all have their independence and their contracts are established in that way. The issue is delicate because we can make some interpretations favourable to consumers but always without removing a contractual clause. Unfortunately, the justice system does not work as well and we would like, and there are many things that we cannot recommend or execute.

EXPERIENCES PANEL OF THE PARTNER CONSUMER ASSOCIATIONS OF THE PROJECT

PRESENTATION ADICAE

Mrs. Paola Pendenza

Italia

Mrs. Simona Spineau

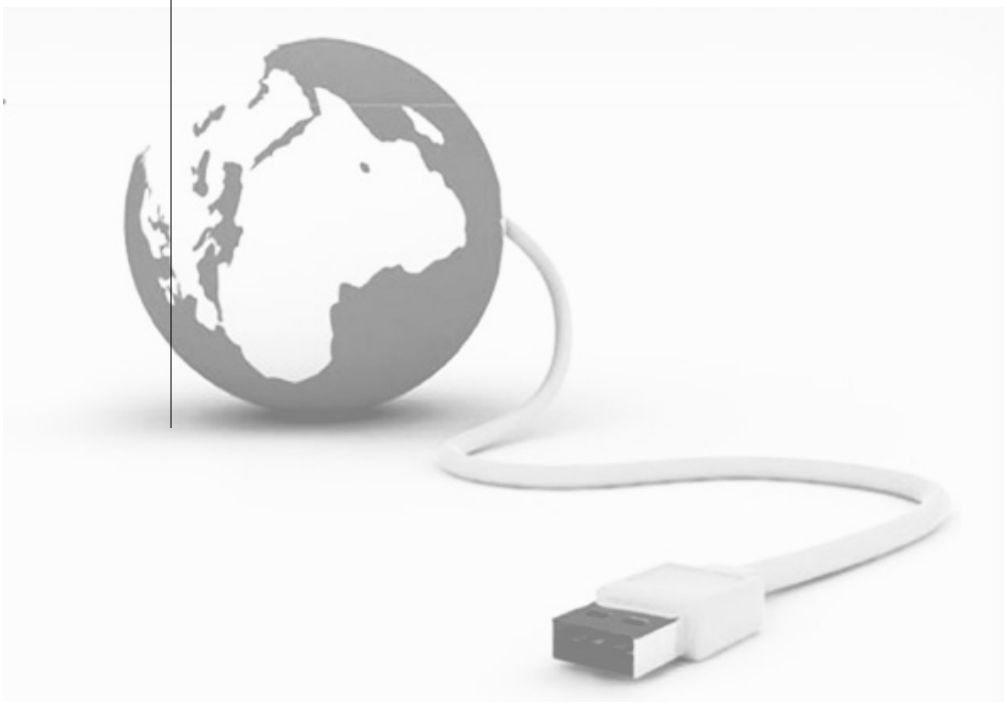
Rumanía

Mrs. Edita Petrauskaite

Lituania

Mr. Miro Túlak:

Eslovakia



EUROPEAN CONSUMERS GIVE THEIR OPINION ON PAYMENT METHOD FRAUD

EXPERIENCES PANEL OF CONSUMER ASSOCIATIONS WHO ARE PARTNERS IN THIS PROJECT

THE SITUATION AT EUROPEAN

LEVELCurrently, at legislative level, there are serious deficiencies in the legislation that defends consumers in the event of fraud in methods of payment. We did not find, in any conclusive way, or in strong and binding regulations, a limited liability regime for the user of €150, in cases of fraud, only in cases of negligent card use. If this requirement has not been institutionalised or generalised, it is clear that legislation does not guarantee the other basic rights of users of payment methods.

Another of the major problems we encountered is the lack of legislation for electronic banking, which leaves one of the most used method of payment without clear rules (to make payments, transfers or transactions in accounts).

In general, we found legislation that is very favourable toward banks, not because they are expressly favoured, but because it does not guarantee the rights of users in a clear way and

without limitations.

Despite this bleak picture, payment method directives provide a light at the end of the tunnel, so consumers should expect the completion of this process of adapting to national legislation to observe and assess if protection has been improved for users of payment methods.

However, before being transposed to national law, it is unclear if the directive itself will be effective and will bear consumers in mind in terms of new methods of payment such as payment by mobile telephone.

Common issues relating to fraud in the EU

- A few years ago, fraud was committed by individual criminals, computing experts who were more interested in demonstrating the vulnerability of a system than profiting from intrusions. Fraud did not use to have a relationship between some and others. Today, the phenomenon of fraud has changed dramatically and the profile of the criminal has changed: gangs that are well organised, clearly motivated by money, who are very difficult to persecute and punish. These gangs can transform easily and operate from different countries.

This means that the fight against fraud should be carried out with international cooperation from all parties involved. The legislation to be adopted should be initiated in Europe to guarantee uniformity and the resolution of these cases, so that crimes committed in one country that have an international connection can be prosecuted effectively.

- The European Commission's action plans, which have been dealing with this problem for some time now, have become a real weapon against fraud, almost the only one today. It is worth remembering that fraud was in existence from the moment that non-cash methods of payment appeared.

- Groups of experts have been created under the European Commission, including the Payments Systems Market Group and the Financial Services Consumer Group. ADICAE, in association with other consumer associations, has actively participated in them, but the effects of their decisions have not yet reached the public in an effective manner.

- The effects of the implementation of the SEPA for users of payment methods is still unclear, not in relation to technical advantages or costs, but relating to fraud.

- A European level, there has been significant cooperation between police forces through EUROPOL, which coordinates all police efforts in Europe.

The important role of consumer associations and cooperation with other market players Consumer associations are working hard in prevention, training and providing information to

consumers (e.g. ADICAE`s payment services seminars) with the following objectives:

Lobbying for the establishment of a European level fraud watchdog, which is necessary.

Improving mechanisms for the cooperation between the players involved, which is necessary to improve consumer associations' tools in the fight against fraud. This cooperation with other players is fundamental and must take into account the users, otherwise this problem will never be eliminated.

Prevention. Education of consumers is fundamental to confront this problem. Knowledgeable consumers will make it more difficult for the criminal.

Participation of users through their representative associations in the processes of creating laws as this is the only way for consumers to voice their opinions.

Mrs. Paola Pendenza (ADICONSUM Italy)

One element to consider is the increased use of the Internet, which entails an increase in electronic payment services. According to the European barometer of 2008, 41% of Italian consumers have access to the Internet and 23% of households using broadband technology; the percentage increases and we have a breakdown of different members of the family. The youngest use new technology and have more experience.

With respect to online shopping, some 18 million users make purchases online; 70% of these purchases are made with the use of electronic methods. The most popular method of payment is the credit card, also pre-paid cards, PayPal and a small percentage by mobile phone. Only 2% use ATMs. In terms of electronic banking, in 2008, there were more than 10 million online accounts and transfers were made to the value of over €19 million.

Fraud facts about Italy

Regarding fraud statistics, in 2007, there were more than 22,000 cases of fraud, representing a 32% year-on-year increase and €1.012 billion.

There are several common elements, which help to identify the profile of the victims: men between 31 and 40, and in geographical terms, 60% of fraud cases occur in Lazio, Campagne, etc.

Credit card fraud is the most common and also personal loans. There was as increase of 58% and 66% respectively. Another element to bear in mind is the detection time when the victim discovers the perpetrator of the crime. In 93% of cases, the perpetrator remains anonymous and, in 63% of cases, the perpetrator is discovered more than 6 months or even years after the crime has been committed.

Causes and consequences

New technology offers more opportunities to commit fraud as the profile of crime has evolved
into an organised crime structure and, finally, we must not ignore the limited knowledge on the part of consumers and their lack of precautions. New forms of communication such as social networking platforms are a veritable market of personal matters and private information.

In terms of consequences, consumers have different burdens. Firstly, with regard to financial losses, but also in the time that users have to spend making a report to the authorities and dealing with the perpetrators. It is interesting to include the concept of psychological and reputational damage, as in most cases, there is also identity theft, which causes harm from a psychological point of view. Fraud is also a burden for companies and card issuers in terms of reputation following fraud.

Possible solutions for an effective fight against fraud must involve the police, banks and consumers. With reference to best practice, I would like to make mention of the main office of
payment method fraud, which is part of the Ministry of Economy and Finance and has been operating since December 2008, which monitors a credit database to prevent and combat credit card fraud and thus provide consumers and card issuers with a protection system, with immediate information about suspicious credit card transactions.

With regard to the activities of ADICONSUM, the association has signed several procedure rules with the main credit systems to help consumers and verify their personal credit data; moreover; various guides on fraud and identity theft have been published to provide support to consumers, and, since 2008 ADICONSUM has participated in a monitoring programme with an Italian company.

Mrs. Simona Spineau (ANPCPPS Romania)

Aspects of fraud in Romania

As in other countries, the cost of financial fraud is high. 50% of computer crime is related to electronic payment systems and most of the fraud targets bank customers. Also, the number of cases relating to cards has increased in recent years; the main methods are phishing and skimming, and the criminals benefit from the lack of security measures offered by banks. Romanian banks are often victims of such fraudulent attacks; with respect to electronic commerce, fraudulent activities originate in Romania but the victims are usually foreigners. There is a continuing specialisation in new technology, using fraudulent electronic commerce phishing websites.

As a result of the main seminar organised as part of ADICAE's project, a new working group has been created, involving all interested parties. A working framework has been established and we hope to provide good solutions to address the problem of fraud in payment methods.

Mrs. Edita Petrauskaite (LNCF Lithuania)

In Lithuania, there are also a growing number of Internet users as well as an increase in fraud. Banks are reluctant to attend our events or provide us with contracts to review and discuss.

Electronic payment cards are threatened by phishing or skimming. It is therefore necessary to improve legislation in order to create a national cyber security strategy to strengthen cooperation.

The latest trend in fraud is withdrawing money from ATMs by tampering with the slot through which cash is dispensed so that the machine does not recognise that it has given you money or if it has remained there; when the card is removed, the money remains in the account but the criminal gets the money and the bank suffers the loss.

Another type of fraud that is popular at the moment occurs when a bill is stolen from the post and is replaced by another with the criminal's account number meaning that the service is not paid for.

Mr. Miro Túlak (ASC Slovakia)

Types of fraud are very similar in all eastern European countries and new members.

The problems are extremely serious and we are lagging behind because a third of the Slovak population does not have a bank account. We have a low level of fraud but, in 2005, the ratio of consumer debt with respect to GDP in Slovakia was 8.9%. Slovakia therefore has much to learn about this type of initiative as we are lagging behind market trends.

We have more time to inform consumers, launch information campaigns, and prepare consumers to protect them against these problems.

In our 16 consumer centres, we deal with financial problems and attempt to solve them, as banks are often unwilling to cooperate with consumer associations.

Mr Asen Nenov (BNAP Bulgaria)

The resolution of conflicts amontg financial entities and consumers in Bulgaria (for cases of fraud in means of payment, or disputes if any kind) has been notewothly increased by the creation of the Payment Disputes Conciliation Commission.

It is one of the tools for out-of-court conflict resolutions in Bulgaria. It is an independent body, consisting of two representatives of the Commercial Banks Association and two representatives of the Consumer Protection Commission.

The chairman is a representative of the Bulgarian National Bank, i.e. he or she is not committed to neither of the both sides of the dispute. .

Mr. Federico Regaldo (MDC Italia)

A very important issue to take into account in the topic of fraud cashless means of payment (leaving aside the enormous increase of the cases and their importance) is that these problems don't affect in the same way all the consumers. The most likely potential victims of this kind of cyber crime are men, aging from 30 to 49 years-old, as they have good credit potentials and as they – more than the others – produce and leave so-called “personal traces” due to their living habits (such as travelling, booking hotels, dining out, purchase goods, requesting loans, etc.).

Professionals in their thirties and forties should pay more attention to certain minimal precautions: according to the above-mentioned statistics, less than 35% of this range of population destroys documents before throwing them into the dustbin and only 37%, on average, currently checks banking statements.

Finally, a very concerning data is that the time of discovery of the fraud, by the victim, is usually very long: on average, it amounts to 206 days; 580 in case of issuing of a credit card and 103 days in case of loan for purchasing goods, with simultaneous issuance of a credit card.

A NEW COMPUTER OFFENDER´S PROFILE : ARE COMSUMERS PROTECTED AGAINST THEM?

FRAUD GENERAL OUTLOOK AND MAIN PROBLEMS FOR CONSUMERS

Mr. Victor Domingo Prieto

President of Internet Users Association

THE NEW "ON-LINE" CRIME PROFILE

Mr. Victor Lorca Báez

Pre-sale Advisor for Panda Security

PUBLIC SECTOR MEASURES TO AVOID FRAUD

Mrs. Dña. Elena García Díez

INTECO E-fraud Area Coordinator

PARTIAL SOLUTIONS FROM THE PRIVATE SECTOR

Mr. Carlos López

Responsible for Optima Web Projects (ANETCOM)

A NEW COMPUTER OFFENDER´S PROFILE: ARE CONSUMERS PROTECTED AGAINST THEM?

Mr. Victor Domingo Prieto

President of Internet Users Association

Fraud general outlook and main problems for consumers

In order to carry out a good analysis of internet reality one must feel a "net dweller" and at internautas.org, we have been performing internet security campaigns since 2002. Initially, in these campaigns we focused on viruses, PC connections ports, firewalls and spam, as they were the main problems at that time, and which are still an issue nowadays.

In December 2004 we discovered phishing and in 2005 around 900,000 types of different attacks were reported. The information provided through our website is the main weapon to fight type of fraud, which although rudimentary and badly described at that time, it managed to catch victims who would provide their personal data.

Initially, banks rejected to inform, on their websites, about phishing and this issue was left in the hands of the authorities, and specially in charge of consumers associations and private initiatives about informing consumers about these types of fraud.

In 2006 there was information about a series of issues:

-Phishing. Detection of an organized band still to be found.

-Fake websites for mobile phone top-ups.

-Fake job offers or "muleros".

-Phishing car. Fraud related to internet car sales.

-Fake lottery. Having, among the victims, people who hadn´t even bought lottery tickets.

Lastly, some reflection: there are laws for everything, even for electronic commerce however what doesn´t seem to improve is the speed in justice. In cases of identity theft, for instance, the speed to avoid more serious fraud is essential. We are demanding more specific courts and in the near future to have "on-line" courts.

Decalogue for child protection on the internet

From our associations we point out the serious problem of child protection, a problem on the increase as parents and teachers do not know well the tools that the internet can provide.

In order to help them, a Decalogue gathering the following advice should be taken into account:

1. Internet leaves traces of internet usage.

2. It is a communication system which has been elaborated by people.
You should be as cautious and respectful with it as you would with a stranger.

3. Do not trust what you would not trust in real life.

4. The information you find on the internet must be compared.

5. Always ask an adult for advice before you take the first steps.

6. Internet keeps all the information we provide about ourselves. Do not provide too much information.

7. Internet is parallel and not unrelated to real life.

8. Internet allows the management of money without touching it. Transactions must always be carried out through Banks/Savings Banks or State Public Administrations.

9. On the internet there is more data than we can assume, therefore we must filter it.

10. There are laws protecting users from people misusing their personal data in order to protect their intimacy, their personal data…

THE NEW "ON-LINE" OFFENDER PROFILE

Mr. Victor Lorca Báez

Presale Advisor for Panda Security

Security professionals have clear that today there are more samples and varieties of viruses than ever before. Additionally, the "ethical hacker" has remained in the background, while the rest of virus creators have realized there is a succulent loot to get, by simply distributing malicious specific codes. In fact, there are authentic mafias dedicated to computer crime and an "underground" market where to buy and sell malicious codes, attacks of denegation of "`a la carte" services or mail listings to send "spam".

This malware creation movement, even targeting specific companies and/or users, is one of the main problems we are facing. Currently, antivirus laboratories are subject to a constant shower of new types and therefore are being inundated. Panda laboratories received in 2008, as many types as the total in the past 10 years, reaching 15.000.000 types.

Making a fast calculation, we can obtain an average of over 40,000 daily samples, when a few years ago we would talk about 30 or 40 per week.

Traditional methods against fraud are now starting to be outdated

Some sector companies tried to alleviate this avalanche by contracting analysts, but it wasn´t long until it was evident that it was not a question of human resources specializing in this task, as soon they were exceeded by the huge amount of new samples. Apart from that, the level of sophistication used by criminals has increased notably as they use now techniques that allow their creation to go unnoticed for as long as possible.

Traditional detection techniques have been questioned for a long while based on company data bases, considering that it is essential for an acceptable type of security to have techniques that can anticipate unknown codes and HIPS systems, besides by following this philosophy of innovation, we have been developing, since 2006, the concept of "COLLECTIVE INTELLIGENCE".

Collective intelligence works as a security platform and as an online service (SaaS) in real time. Mainly, it is based on five principles:

1. Taking advantage of collective knowledge to proactively protect others.
2. Automation and improvement of collection, classification and malware elimination.
3. Acquisition of knowledge on techniques to improve the existing ones.
4. Use of a proactive technology generation from the cloud computing.
5. Distribution of a new generation of proactive services from the cloud computing.

All in all, this model allows us to detect more quantity, faster and to distribute solutions more effectively.

Do entities and companies effectively protect themselves against fraud?

On the other hand, when a company decides to carry out the implantation of a security solution which covers the main needs in the best way possible, then three basic aspects are to be taken into account.

1. How long is the implantation, display and configuration going to take?
2. How much is the solution going to cost?
3. Simplicity in the solution management.

Obviously, any of the three factors are essential.

Taking into account that in Spanish companies the figure of a security administrator, exclusively devoted to this issue, is practically inexistent, the possibility of having a solution which is integrally managed by specialists becomes quite attractive, and even more if it contributes to the reduction of costs related to the additional infrastructure required by security solutions.

In the context of this case, we can propose SaaS solutions, which provides the mentioned benefits, as the whole infrastructure is hosted on the service provider.

In the specific case of Spam, the SaaS solutions also provide important saving in the band width available for mail. Taking into account that approximately 85% of email on the internet is spam, the elimination of that unsolicited traffic allows the optimization of the company´s communication.

Right then, the figure of the managed security service provider becomes relevant (MSSP), which offer services 24X7 from technical personnel highly specialized in security. Trusting this type of solutions give companies the opportunity to optimize the cost of the solution, reducing to the minimum the budget for hardware and personnel training and allowing economic resources to be spent on other aspects. Unfortunately, they are not well implemented or spread currently and users continue unprotected based on traditional methods.

MEASURE OF THE PUBLIC SECTOR TO AVOID FRAUD

Mrs.Elena García Díez

Inteco e-Fraud Area Coordinator

The development of the Information Society is shown not only in the increase of the number of internet users, but also through a clear diversification of services offered on the net. Bank operations, administrative processes and all types of purchases related to the traditional search for information as services frequently used on the internet.

Within this context, the user accesses these new services while, for instance, Research on fraud practice known as phishing published by the Information Security Observatory of INTECO gives data about its knowledge level regarding terms related to electronic fraud. From the results of the Home panel, also a result from the work carried out by the Information Security Observatory, whose results allowed us to improve our diagnosis by means of data on how to use security tools at home and specially about user´s habits, emphasizing a low interaction level with these tools, and attitude clearly contrary to the urgency with which anyone would change their home´s locks if they had found out they doesn't lock properly.

This diagnosis can be completed making reference, firstly, to the investment of companies which render their services, a priori more sensitive to possible electronic fraud as it is internet commerce or banking, with the aim to obtain a safe development for their own objectives and secondly to the consequent evolution of all threads that are present on the internet which gain in sophistication both technically as well as in social engineering with the aim to impact in what is still the weakest link, the user.

This situation means a challenge for all sectors and actors related, from the industry to entities as efforts and solutions developed, apart from protecting against the evolution of internet hazards, must get to the final user together with the information and training allowing the use of all on-line services within a security and trust culture framework.

There are different publications making reference to technical and resources specifications which support electronic fraud attacks in Spain, but none of them allows a complete diagnosis on which to build new strategies to fight against these activities, as they are performed isolated and not based on the total registered incidents as there is no knowledge base centralized with the data of all actors and entities.

From the security incident service for small and medium businesses and citizens of INTECO, rendered from INTECOCERT, we can also observe the complexity of new incidents and the degree of knowledge with which citizens face them. These incidents encompass from phishing cases, which are frequently supported in dynamic and intelligent systems to intrusions on websites of small commerce which make them into involuntary diffusers of marketing content.

Aware of this problematic issue, it is necessary to collaborate in the generation of a security culture type accessible for all citizens by means of information for active protection of users is proposed under a range of reference, free useful security tools, software updates and sections offering specific protection means for groups such as child protection on the internet.

Besides, reporting incidents as well as managing them is fundamental, a service provided by Inteco and by any consumers´ association, and lastly, continuous updating about new types of fraud by means of bipolar communication with users, who, after all, are the most common victims of this type of crime.

Inteco offers all the information available for Forces and Security Bodies in order to try and provide a support tool for their investigation tasks and crime prosecution.

All in all, the first tool we must put in the hands of citizens to make them stronger when facing any type of electronic fraud is a culture of security to safely exploit the advantages that the internet can offer. Apart from that, if from the administration as well as from the industry and related entities start up new technologies based on collaboration and experience we will be ready to provide the market with new solutions adapted to the current times.

More direct collaboration between INTECO and financial entities is missing as we do not know how much they support or receive information about this data base and also with the citizens, either directly, or by means of their most representative consumers´ associations

(for instance those forming part of the Consumers and Users Board).

SPARTIAL SOLUTIONS FROM THE PRIVATE SECTOR

Mr. Carlos López

Responsible for Optima Web Proyects (Anetcom)

No doubt that e-commerce, that is, commercial transactions performed on the internet as a background, are experiencing a immense increase recently. With figures in hand, we can see an increase of nearly 20% a year, in the period between 2002-2006. This increase doubles in 2007 to reach nearly 5,000 million €, which places us at the head of Europe.

Also, we must emphasize that the profile of the internet user is changing radically, as today there are more than 7 million “internet buyers”, or internet users performing internet transactions, which means almost 40% of current internet users. Therefore, we are facing an increasing market, although it would be better to consider it a facilitating environment for those commercial transactions which constitute the e-commerce global market.

We are experiencing such an extraordinary growth that it is virtually impossible for a Legislative branch in Spain, with a structure and functioning typical of the 20th century, to legislate in order to establish a legal framework for commercial relationships to be established, in the same way as they are carried out in the real world but with an important cost reduction, which confers it a tangible comparative advantage with this world that is so real, physical and at the same time so reduced, with limited actors dominating as they grow bigger and that also control the distribution channels.

Here is where the great difference lies on the internet: freedom and equality.

We are all equal on the internet, we have the possibility to trade on a large scale with a less infrastructure than the traditional company, we can externalize logistics and other additional services in order to pay attention only to the core of our business.

In the current legal situation we rely on auto-regulation on this matter. In this frame of mind, ANETCOM, a non-profit private entity in the Community of Valencia develops a Project called “Optimum Web”, based on these three main pillars:

- Transparency, Security, Confidentiality in communications (LSSI-CE, LOPD).
- Usability and Accessibility for people with disabilities (AA According to WAI of W3C).
- Child protection by means of content classification systems.
- Extrajudicial conflict resolution by means of consumer arbitration boards.

The "extension of legal guarantees" of users appear in the quality stamp´s pillars (number one, two and three). The so-called usability, a term which refers to facility and simplicity of usage on a web portal, as well as its accessibility gather an increasing tendency.

Regarding child protection, when from the audit the offered products or services are detected not to be adequate for those who are under age, the company is urged to install content classification systems in a way that they can assure that the person accessing the content is above the age of consent.

One of the main advantages is the those companies adopting "Óptima Web" (Optimum Web) will automatically be adhered to the Consumer Arbitration System, as any other conventional type of commerce, in a way that complaints can be solved through the Consumer Arbitration Boards instead of using legal channels, which is a much slower process. Even some type of private mediation could be expected before the intervention of the Arbitration Boards.

If “Confianza Online” (On-line Trust) the other great commercial stamp is oriented towards big corporations, at Óptima Web (Optimum Web), this stamp is intended to be for PYMES (Medium and Small companies) e-commerce. Its fusion would fill an empty space in Spain, which in other countries take up brands such as E-trust o Webtrust, entirely necessary for the final consumer to associate it with a logotype, a stamp or distinctive with high quality standards, which allow everybody to purchase and sell on the internet without any worries.

THE CONSUMERS´ VOICE: QUESTIONS AND REFLECTIONS

P: Should there not be more promotion by public administrations so that the stamp is recognized?

R: The problem is that it is a political conflict. There is an official stamp from Red.es which means “On-line trust”, but it is a stamp for big companies.

P: Does the stamp guarantee good website functionality of the sites we surf?

R: The stamp audits that the users´ data are duly treated and that the payment gateway is correct. The only thing that can not be taken into account is the user´s computer.

P: You have mentioned that every two years there are audits, is that not a long time?

R: There are internal controls carried out at shorter intervals.

At the end of each one of the Panels, there were interesting debates included to the Minutes of this Symposium

ELECTRONIC BANKING. ARE CONSUMERS SAFE?

THREATS MULTIPLY. PRACTICAL OUTLOOK FOR FREQUENT TYPES OF FRAUD.

Mr. Vicente Díaz

Intelligence Fraud Manager Support SEC21

ELECTRONIC BANKING. ARE CONSUMERS SAFE?

Mr. Agenor Gómez

Responsible for ADICAE Legal Services

MEASURES FROM THE PUBLIC SECTOR TO AVOID FRAUD.

Mrs. Lucía Palacín Prieto

Director of Electronic Banking and La Caixa New Technologies Legal Consultancy

THREATS MULTIPLY. PRACTICAL OUTLOOK FOR MOST COMMON TYPES OF FRAUD.

Mr. Vicente Díaz

Intelligence Fraud Manager Support SEC21

It is important to technically distinguish between the two sides of communication: the user´s side and the entity´s side. In the last few years, financial entities have made an effort concerning security, taking conscience of the damage caused by fraud for their expansion pretentions and they are devoting, little by little, resources both to safe development, audits, etc. The weakest link today is the user as we are all vulnerable at any time. We have to be conscious that from 2005 the cybernetic mafia issue moves more money than drug dealing, to give an example. It is not only the users' responsibility but also the entities´.

New threats and insufficient protection

Security products such as antivirus, etc. is necessary but not enough; it is true that it is impossible to obtain 100% safety against all threats. For instance, an antivirus is protecting us against 90 % but the worrying issue is that the remaining 10% is the one giving way to fraud against consumers.

User education is proposed as a very important challenge, however, we must think about that 10% margin being solved in this way.

The question is that all browsers are vulnerable; the typical piece of advice about not surfing doubtful origin websites is no longer of use as it is a fact that in the last year, for example, numerous attacks have been carried out in legitimate webs after finding vulnerabilities that these had and inject malicious codes that would redirect us to their pages in a totally transparent way so that the user ended up infected. The user might be visiting their favourite online newspaper and get infected because that website has got infected. Here, the responsibility is not the user´s due to not being protected. Fraud is nobody´s responsibility but an economic and social problem consumers can not be responsible for as all technological, criminal questions, etc. exceed them. Concerning email is where, perhaps, there is a higher conscience, in those emails we received that are fraudulent.

Mafias can see our desktop data that we have, recover files or even format our equipment.... a series of actions to obtain an economic return from those infections; this way we realize that this is really a business and all these infected computer nets are exploited always in damage of those affected.

Many of the trojans around are banking trojans asking us for our bank details and to send them to a third server. Bank details have a price and their traffic significantly enriches mafias. And, to a certain extent, the person who "creates" the trojan, very often, sells it and it is the crime band the one operating with it.

Another issue is that "home routers" are being attacks in our homes; they are cheap products provided by internet distributors with not much security and therefore, the virtual objective is any sort of "malware".

Massive infections are on the increase as they inexpensive and this way they get a very high ration of consumers affected indiscriminately.

Education and....something else?

The most important thing is the education and awareness of users; education is more difficult but an effort must be made in order to know the basic tools that we can use to defend ourselves.

The more difficulties and obstacles the user can make to avoid fraud, the better the situation will be, we need to be aware that we will never be completely protected. More transparency is needed and we have to inform our entity if we see any suspicious operation on our computer.

ON-LINE BANKING, I S THE CONSUMER SAFE?

Mr. Agenor Gómez

Head of Judicial Services at ADICAE

Before On-line banking

In the early days of on-line banking, the traditional financial entities were not very supportive of this style of business, indeed, in its earliest days, on-line banking was conceived as a separate project: Organisations began to appear that used the "Click" business model, which is completely virtual, with no offices, meaning that the client carries out all his banking operations online. In Spain, at the beginning of the millennium, a foreign financial body launched a new, high-return, commission-free operation for deposits that revolutionised the traditional marketplace.

In general, this model did not achieve the mass acceptance it sought from clients mainly because of the barriers that still created a certain lack of confidence, security and depersonalisation of the client-banker relationship. Faced with the exponential growth of traditional banking costs, this type of simple, low-cost service has occupied a niche in the marketplace and has driven the larger traditional banking concerns to enter the Web-based financial world through totally virtual offices.

However, the "Click" model still does not count on the total support and confidence of the client, who still prefers to visit his office to carry out the majority of his operations.

The first and fastest expansion

After the technological bubble burst, most projects based on a "Click" model were closed down and a new model was adopted known as "Click&mortar" which efficiently combines the physical services–offered at the local office-with the online services which the client is free to choose between. This is the model which has become more popular, due to the lower costs involved in using a virtual office. Apart from this, the use of Internet is free to the client so he does not have to bear the heavy financial burden that the traditional banks have incurred, so the opening and maintenance of on-line accounts or on-line banking are free of charge. Added to this, the immigration phenomenon, with the resulting growth in foreign populations within EU member states, economic progress, the internationalisation of social and economic relationships and the unstoppable development of universal Internet access is a great leap forward and huge opportunity for the growth of on-line banking.

The adaptation to the new social, cultural and economic order in Europe is the predominant factor in plans for the development of On-line banking. We live in a technological society, where a new generation is imposing itself, where the use of technology is becoming interlaced with daily life. As Internet becomes more common in homes, On-line banking will develop at a pace: if Sweden, Holland and France have the highest growth in homes connected to the Web, it follows that they also present the greatest percentage of On-line banking users.

The client counts: Confidence and security

Confidence rates highly among the keys to the development of on-line banking. Consumer securIty is one of the main keys to gaining the confidence of the client.

Every survey carried out since 2006 shows a loss of client confidence in on-line banking, as a result of the huge number fraudulent attacks –phishing, keylogging or vishing-. The consumers who are surveyed always demand a safer authentification system - one that goes beyond a mere password.

Do dependable technological solutions exist?

Industry technicians and spokespersons who represent companies involved in developing on-line fraud protection systems claim they are always one step behind the hacker and that it is impossible to offer a 100% safe solution against every conceivable form of cyber attack. They further confirm that every format is vulnerable.

It would appear impossible to protect a consumer using the latest personal computer, equipped with the most advanced domestic protection software available from the hacker who is trying to impersonate the client in the on-line banking world:

What can the consumer do against a coordinated attack by a hacker using a "zombi" computer?

It would appear evident that whoever offers the ser-

vice and supplies the means (the banks) must also invest in the highest and most advanced levels of security available in the on-line banking systems. It is they who have the financial and technological capacity to do so. The client can do no more than use the technology available to him. This links into the growth in costs that goes hand in hand with the growth in popularity of on-line banking.

If initially, the use of on-line banking was driven by a reduction in costs, (free transfers etc) nowadays it isn't that this cost reduction no longer exists but that the use of an on-line banking service brings with it a maintenance cost. This is the consequence to the client of the current liquidity crisis:

The current model is to capture client's accounts by offering incentives: one current campaign announces a special interest repayment for a new free on-line account, but only during the first year, after which the cost is 9€ a year.

Transferral of costs to the consumer of a fraudulent operation

The lack of client confidence has grown even greater due the perception that in the case of a fraud being carried out, then it is the client who would be liable for the loss.

This perception derives from the attitude of the banking entities when faced with complaints by a client in the case of an on-line banking fraud: This stems from the position taken by the banks of blaming the client and transferring the economic consequences of a fault in the internal security system to him.

You only have to glance over the small print of a contract for an on-line banking account to realise how the banks are trying to proportion the blame for fraud firmly at the client's door. The client will have to bear the responsibility of proving that he has not been negligent with respect to the security of his passwords.

Legislation is patchy and deficient, but the courts are beginning to favour clients.

The Banco de España decided in favour of a client in a Phishing case in 2006 with the following decision:

"Having looked at the documentation (among which is the contract for on-line banking) it must be remembered that the Building society had facilitated all the necessary warnings to avoid on-line fraud before the controversial transfers took place"

Even so, the bank had still refused to repay the more than 6000€ that the victim had lost, which gave rise to legal proceedings which finished with a ruling against the bank. (Sentence of the 25th June 2008 in the first Law Court nº 2, Castellón, Civil Case 345/2007) in whose findings can be read the following:

"In General Stipulation V, it is clear that Bank… was exonerated of the fraudulent use of identification keys because of user fraudulence or negligence.

SIXTH.- As stated by the SAP in Madrid, Section 13, 11th February 2005 (EDJ 2005/69542), the clauses referred to displace the bank's responsibility to the client who played no part in the damages caused, infringing the content of clause 14 of the First Amendment to the General Law for the Defence of Consumers and Users insofar as it imposes limits on the consumer's rights.

In fact, it is not a given to impose upon the consumer the indiscriminate rejection of the right to complain to the bank who supplied him with the necessary technical means for better or more convenient services, in those cases where, being unworthy of consideration as a one off case or of force major they are effectively not attributable to the bank, yet do however cause damages."

Electronic signature for on-line banking

The penetration of electronic signatures or DNI, driven by the Information Society and which will permit the complete contracting of on-line banking services, is practically nonexistent, mainly because of the claims by the very banking entities who use it, that the use of an e-signature has been, in their opinion, a failure.

This has lead to the use of an e-signature as a form of identification to become almost anecdotal, as the majority of the banking institutions do not even include it as an option to access on-line banking accounts.

Apart from this, there is a general lack of knowledge among the public of the value of this option and how you apply for one.

This is mainly due to the fact that there is no coordinated promotion campaign for e-signatures nor instructions on how to go about obtaining one from a financial institution. This could be the first step to creating a truly virtual office, a business model in which the client has complete freedom and security to choose between managing his accounts on-line or in an office.

CONCLUSIONS

1.- NEW ECONOMIC MODEL: The economic cycle change from expansion to contraction will introduce a new business model. Whereas in the previous period of rapid growth banks tended to increase their retail sales operations with numerous regional offices being opened, in the current climate of restructuring of banks with fusions, absorptions and dissolutions, the efficiency brought about by cost reduction could lead to a new on-line banking model under the "Click&mortar" model, which could lead to lower transaction costs and higher customer satisfaction.

2.- EFFICIENT COMPLAINTS PROCEDURES: As well as the fact that on-line services should offer substantial costs savings, the majority of on-line bodies do not have an efficient complaints procedure to respond to clients' problems. To rectify this, the financial entities would have to undertake heavy investment in the necessary technology to supply safe systems to increase client confidence in on-line banking. E-security must be provided by the supplier and not the user.

The financial entities must provide the legal and technical measures necessary for the implementation of an e-signature that is recognised by the banks, and must adopt any additional measures to help the outdated and simple key card (a combination of SMS or other type of identification).

3.- EFFICIENT AND PROTECTIVE LEGISLATION FOR THE CLIENT AGAINST FRAUD: The client protection doctrine of the courts must be transformed into laws in the case of e-fraud in order to overcome the lack of consumer confidence. The philosophy must become one of preventing the translation of the cost of the fraud to the client by the financial body concerned. This could become an acceptance of responsibility by the institution who supplies the service to the client, imposing upon the financial institution the obligation of efficient and updated information on every aspect of the use of the service, in such a way as to ensure that the client will always be exonerated from blame in a fraud case, unless the financial institution can prove that negligence took place in the use of the service, thus transferring the onus of proof from the client to the bank.

Image of the conference hall during the speech of Mr. Agenor Gómez, lawyer of ADICAE

ANTI-FRAUD MEASURES WITHIN THE PUBLIC SECTOR

Mrs. Lucía Palacín Prieto

Director, Judicial Assessor, on-line banking and New Technologies, La Caixa

The importance of Internet in the financial sector is enormous, as data from 2008 shows which says that 45% of users use financial services on-line, which equates to 17% of bank customers. Today, a financial body can offer up to 700 different operations by Internet, ranking from consultancy, which was the beginning of on-line banking, to service contracting (loans). If we take a moment to think about these numbers, this means that the banks have another distribution network to add to the traditional ones, and which permits greater accessibility, speed and convenience, 24 hours a day, 7 days a week but that which requires from the client a familiarity with Internet and its tools. These advantages have brought about an increase in services to the client and a reduction in costs for the financial institution as new services and providers come on line.

The down side is on-line fraud, the new forms of criminality that have arisen with the use of Internet in financial services and the importance of international transactions, fraudulent operators and globalisation.

When talking about security, we can distinguish between three conceptual environments:

-The legal and contractual application of these guarantees which are currently offered by the EU.

-Fraud prevention elements.

-Responsibility, once the fraud has occurred and the persecution of the perpetrators.

A) Legal and contractual: In 2007, a law was passed that deals with party's obligations and due caution that a financial institution must observe when offering services on-line, whether talking about distance contracting or the appropriateness of services; This was added to the already existing laws established in 2002 which brought about the Laws of the Information Society and e-business.

The e-signature laws are a guarantee of the declarations made when conducting business on-line: as far as the Information Society is concerned, there is a voluntary law from 2007 which modifies a set of laws and, in addition, adds certain obligations to companies and financial entities.

The Internet boom of 2000 saw many projects operating in an enormous sea of legal uncertainty.

There were no laws to protect contracting on-line, and the financial institutions based their activities on a type of pact that has become, with the passage of time, the typical contract for on-line banking.

When, in 2002, the e-business law recognised the validity of on-line contracting, these contracts continued in use as a way of offering a greater transparency in relationships, information about the risks of misuse of Internet tools and the obligations that the consumer had and still has, when there is a suspicion of fraudulent activity by a third party.

Over the last 9 years, there has been a transition from a consultancy service to a vastly varied operation which completely covers every aspect of banking, with the exception of those services that, by law, may not be contracted on-line. Also within the scope of security, there has been a transition from a single PIN to a second PIN with signature, which is necessary when establishing new contractual relationships or to confirm economic operations that involve the accounts of the client.

Firm user rights

Firm protection that the distance financial services law grants to clients includes the obligation that the financial institution has to provide clients with all the pre-contractual information necessary. As well as this, that the information is available on media that the client can download directly to his computer, and in a paper format; a right was also added for a cooling off period when buying a product or service through Internet of 15 days or 30 days for insurance transactions, except when specifically excluded.

In addition to this is the protection afforded to clients when a credit card has been fraudulently used on-line; the client can demand the immediate cancellation of the operation; it also includes the prohibition of supplying non-solicited services, and most importantly for the financial institutions, is the risk that their own laws establish, that a contract can be considered null and void if it does not meet all of the previous information obligations. All this naturally falls to the financial institution to prove.

B) Protection and prevention: Protection is afforded in two distinct ways:

-Institutions must identify efficiently and truly the client on the first operation, not only because all subsequent operations will be attributed to him but because there are rules in place to prevent money laundering, data protection and because market relations require it.

E-signatures have not been implemented yet in the world market and new systems of identification are being studied by the financial institutions with very promising results.

Indirect elements are being used, such as the security within the installation and multi-channel security, a limit to

the number of institutions etc. This does not attack the root of the problem but serves to mitigate the possible risks. The client is the one who establishes these limits for particular operations.

-Finally, one very important element is the sharing of security concepts between clients-consumers, and the banks are considering making this obligatory; to achieve this, sharing within Internet is of vital importance. The financial institutions are obliged to inform users of security measures in Internet and the users are obliged in turn to understand and use the tool.

Precautions:

- Never supply personal information or PIN codes.
- Never open un-solicited emails.
- Never give personal data to a third party or open unknown files.
- Never write down PINs.
- Never be tempted by offers or gifts.

PC security measures are important.

c) Crime prevention: from a risk point of view, cybercrime has evolved into new types of crime whose aim is to steal access codes in order to fraudulently obtain money by tricks and techniques such as Trojan Horses.

The key to cracking this type of crime is to prevent this type of conduct and to prosecute the crimes and their perpetrators, the Networks are complex and extensive and are located in various countries, which means there is also the problem of jurisdiction and the sovereign penal system in each country. The only way forward is through cooperation among countries.

Sentences and responsibilities related to phishing;

In a phishing scam, a lot of people are involved in the crime although some may not know the full extent of the operation, and based on that fact, the traffickers had been declared innocent of responsibility until a High Court ruling in 2007 admitted this responsibility. A court in Castellón considered the financial institution guilty because it took too long in reporting the attack and so was considered to have aided and abetted the crime. A sentence on the 10 of March 2009 declared concurrent guilt, because the client facilitated the PIN numbers and the bank did not notify them in time.

THE CONSUMERS' VOICE: QUESTIONS AND REFLECTIONS

Lucia Palacin: I'd like to answer my colleague, the failure of the e-signature is well known. It is one thing to send a tax return through Internet and quite another to transfer money from one account to another. They are very different and the risk level is distinct.

The client must know what he is doing, of course what we cannot do is assume that all of the risk must always lie with the institution, because if we did that, the client would never worry about a thing.

P- If a standing order is put on your account that you haven't requested, you can refuse to pay it, right?

R- Of course you can if you didn't request it. It is impossible to charge it to your account without the e-signature. (Lucia)

R- What you can do is to set up a standing order and if you don't check your statements and you miss the payment, you can't get it back, that's why now on some invoices the account number appears between asterisks. What I mean to say is the responsibility in the case of a fraud does not get transferred to the client who acted diligently but is the responsibility of the financial institution. The institution must always respond unless it is obvious that the client did not act correctly. That's why I said that the necessary measures must be in place, to avoid this happening. (Agenor)

ROUND TABLE: CONCLUSIONS ON THE CONSUMER'S POSITION IN THE CASE OF FRAUD

EXPERIENCE PANEL WITH THE PARTICIPATION OF THE FOLLOWING CONSUMER ASSOCIATIONS:

Bulgaria: "Consumers' national Bulgarian Association (BNAP)"

Eslovaquia: "Consumers' national Slovakian Association (ASC)"

Eslovenia: "Consumers' national Slovene Association (MIPOR)"

Italia: "Associazione per la difesa de consumatori e ambiente (ADICONSUM)" "Movimiento Difesa del Cittadino (MDC)"

Lituania: "Lithuanian National Consumer Federation (LNCF)"

República Checa: "Sdružení •eských spot•ebitel• (S•S)"

Rumania: "Asociatia Nationala pentru Protectia onsumatorilor si Promovarea Programelor si Strategiilor din Romania (ANPCPPS)"

MODERA: ADICAE

ROUND TABLE: CONCLUSIONS ON THE CONSUMER'S POSITION IN THE CASE OF FRAUD

Guests: ***Representatives of consumers, financial institutions and public bodies.***

Presenter and moderator: D.Jofre Farrés, ***Secretario General de AICEC-ADICAE***

Moderator: One of the recurring themes has been the responsibility for present and future risks. Of course, advice has been offered to minimise these attacks on security and to reduce the economic impact of fraud that for some is a clear reality and for others is a technical question. One of the first conclusions to be drawn is that payment fraud means "lack of technical measures" to some and "lack of willpower to do things properly" to others, but always being careful to protect the consumer and his rights. We have also seen the measures we have at our disposal to avoid this type of fraud and those we should have in the future; some proposals have been put in motion and others are more curious and innovative. Another conclusion is that responsibility rests on everyone's shoulders and we should remember that. We have to try and ensure that products are contracted securely to try and stop this fraud. Consumers must assume responsibility but they must be correctly informed and given the necessary tools to meet that responsibility

ADICAE

Even the most cautious consumer who takes every conceivable precaution can fall victim to fraud.

Until it isn't guaranteed a total security of the payment instruments; or some actuation standards are given to the user, which don't stablish the burden of proof for the consumer, financial entities must assume the liability in cases of fraud, except particular and very evident cases.

Local consumer information offices

ADICAE should be pleased that the objectives have been met satisfactorily. The collective opinion is that on-line sales and payments improve competitiveness and are convenient but the future for the on-line consumer who is testing the water is unclear and yet he is being invited to jump in.

The consumers who use these new technologies

Just so that it's not all good news, as domestic users we have been quite frightened by what we've heard here at the meeting, by the loopholes that are apparent in the IT world. In the first place, users are not party to the information that has been discussed here and if they were, many would not undertake on-line contracting. Those of us who work in consumer affairs and can see into the future are a little frightened. The most interesting thing has been that the communications channels who permit fraud to happen are the same ones that allow the financial institutions to carry on their business. It's true that we have all recognised the lack of sufficient legal protection that allows this situation to continue; but we must also ask ourselves about the political interest in finding a solution. I think that this international symposium should serve as trampoline to create an international organisation that is capable of taking part in every group where decisions related to these matters are to be made.

The Public Administration representative

Consumer experts are not specialists in these matters, we are quite a long way behind in new technologies and in the question of fraud; these are crimes and administrators have no jurisdiction, although we can make a contribution in information, responsibilities etc. We have to get up to date and act through information and education and of course we have to have much more contact and dialogue with consumer groups.

PART 4

Conclusions

CONCLUSIONS

GENERAL CONCLUSIONS OF THE SYMPOSIUM ON METHODS OF PAYMENT

-A progressive implementation of alternative payment methods in Europe and Spain.

-The exponential growth of alternative payment methods does not equal improved security;

The greater profits gained from an increase in sales are not currently reinvested in greater security measures.

-There is a lack of understanding by the users of electronic payment methods. A large part of the responsibility for this rests with the financial institutions, given that many frauds occur due to lack of information.

-These crimes tend to be international, meaning that there are several jurisdictions which slow procedures and investigation down.

-There is a disparity among laws and investigative procedures between different countries. There is a need for effective coordination between Interpol and Europol.

-The crimes are normally aimed at consumers and this gives rise to the following:

-This is the least protected group as far as information and technical and economic resources are concerned.

-Regulations do not reflect this situation and responsibility still lies with the consumer when there is no information, training or security measures in place to justify this.

-Small scale fraud is prolific and these are often interconnected, but it is this small scale that divides the individual importance and makes them difficult to investigate

(the difference between a crime and petty theft)

-New security measures that have been announced, such as smart cards, have already been targeted for attack by cyber criminals.

PROPOSALS AND CHALLENGES FOR FRAUD ERRADICATION

If growth is more important than security, the financial institutions must accept the problems and loopholes that the use of these payment methods means and assume responsibility unless in a clear case of negligence. Otherwise, insurmountable friction will be caused between the expansion of the payment methods and the placing of responsibility on the consumer.

CONSUMERS

-A need for greater training and information when contracting methods of payment, including teaching material and courses. Consumer associations will participate in the elaboration of these courses.

- The creation of a responsibility standard, which will lay out clearly the responsibility of the consumer insofar as obligations are concerned, providing some basic common rules for payment methods and to ensure that the consumer knows that by breaking these rules, he may well be held accountable for the full amount. With this type of rules, the existing legal insecurity and ambiguity will disappear.

TO FINANCIAL ENTITIES

-Bigger implication in the erradication of the fraud even risking the growth level of the number of transactions and number of clients.

-Elimination of the abusive clauses of contracts using, for this purpose, simplified contract models approved by the National Bank of Spain and where no modifications regarding the liability of the user will be accepted. Consumer Association would also contribute in the drafting of those contract models.

-Hadling to consumers of teaching materials about fraud prevention, fraud simulators, etc. that allow more efficiently to know about the operativity of means of payment.

-Substitution of soft Laws and autorregulation codes for binding and representative norms, which financial entities commit to accomplish for the benefit of consumers.

-Acceptation of consumer arbitration procedures, which should be specialised in fraud in means of payment, in order to avoid the commonly long, problematic and inefficient out-of-court proceedings of conflict resolution existing nowadays.

TO PUBLIC ADMINISTRATION

- Impulse for the creation of teaching units against the fraud in means of payment, with representatives of

- Implementation of out-of-court solution for fraud in means of payment related to consumption. They should be accepted by the entities, and should be specialised with technical and legislative knowledges, so that the resolution of conflicts would be a lot easier.

- Creation of security standards (quality certificates) which would qualify the level of protection offered by a web page (level 1, 2,3, etc). Thay would be awarded by the authorised public administrations and they would warn the user in case the web page isn't secure or hasn't any kind of public control.

- Inspection campaigns of the consumer issues public administration of web pages where goods and services are offered, as well as the verification of the level of security offered to clients who do payments in that webpage. That would be also done for e-Banking.

FOR THE REGULATORS

-Improvement of the out-of-court conflict resolution procedures by the creation of a faster judicial or out- of-court proceeding that permits a easier solution of disputes and improves the confidence of the users in the systems, even in case where there is some economic damage for the consumer

-Supervision of contracts of financial entities in order to avoid the existence of abusive clauses

-Unification of the agreement for clear and less flexible criteria of the legislation in the diverse European countries about

FOR THE LAW ENFORCEMENT AUTHORITIES

-Unification of the procedural legislation and competences at a European level, so thay they allow a faste resolution for conflicts or investigations

-Provision of bigger resources for law enforcement bodies and prosecutors

-Strict application of legislative criteria such as “pro consumatore”, adapted to the means of payment as long as a legislation that properly appoints the responsability of each of the parties isn't issued.

-Creation of common commissions of financial entities and law enforcement authorities where the stakeholders can explain the new trends of criminal and make proposals taken into account by financial entities as well as means of payment issuers in order to avoid the proliferation of frauds

PART 5

Annexe

Regulations

PROVISIONS ISSUED BY THE EU ON THE TRANSPARENCY OF OPERATIONS AND CLIENT PROTECTION

- **Recomendation 88/590/EEC**, by the Commission, 17 November, relating to payment systems and in particular to the relationship between card holders and issuers.

- **Recommendation 87/598/EEC of the commissio**n, of 8 December 1987 on a European Code of Conduct relating to electronic payment (Relations between financial institutions, traders and service establishments, and consumers)

- **Recommendation of the European Communities 17.11.1988**, establishes the responsibility of the issuer for the non-execution or incorrect execution of payment instructions and unauthorised operations by the holder. BUT it is not sufficient to appreciate the lack of execution or negligent execution, but to demand from the card holder does not commit any of the following: fraudulent acts, grave negligence, non-compliance with the clause referring to safekeeping of the card.

- European Code of Good Banking Practice with respect to card payment systems, 14th November 1990.

- **Recommendation 97/489/CE**, by the Commission, 30th July 1997, relating to transactions carried out via e-payment methods (contains the minimum information that a client must be given relating to transactions). NOT BINDING, but important.

- The issuer (E.F) is responsible in the case of non-payment or defective payment of transactions on behalf of the account holder, unauthorised transactions or any error attributable to the issuer related to the management of the account, assuming the financial consequences resulting.

- **Directive 97/5/EC** European Parliament, 27th January 1997, relating to cross-border transfers.

- **Regulation nº 2560/200**1, European Parliament, 19th December 2001, on cross-border transactions in Euros.

- **Framework decision 28th May 200**1, Relating to the fight against fraud and falsification of payments for non-cash transactions.

- **Directive 2007/64/EC**, European Parliament, 13th November 2007, on payment services in the interior market.

- **Directive 2008/48/EC**, European Parliament, 23rd April 2008, relating to consumer credit contracts.

Criminal Code

1. Provisions relating to payment fraud.

2. Who is the victim of a fraud? The financial institution or the account holder?

1. Provisions relating to payment fraud.

•Fraud art. 248.1 CP: "A fraudster is a person who commits a fraud with the intention of obtaining money by trickery to induce another to make an error".

•Electronic Fraud, art. 248.2 CP: "Those who, with intent, and using some form of electronic manipulation, achieve an unauthorised transfer from a third party account".

•The crime of currency falsification according to 386 CP, "Money shall be understood as credit and debit cards, traveller's cheques and legal tender".

•The crime of robbery with force and the crime of robbery of objects with force, art. 238 CP, in the case of the use of a credit card and number to extract money from an automatic teller.

•The crime of revealing secrets, art. 197.1 y 2 CP relating to crimes against IT security and fraud known as "Hacking and Cracking":

"1. A person who reveals secrets or damages the privacy of another, without prior consent, and who gains accesss to his papers, letters, messages, e-mail or any other type of document or personal effects or intercepts his communications or uses listening, transmission, recording or sound/vision reproduction apparatus or any other type of communication signal apparatus will be sentenced to a term of imprisonment of between 1 and 4 years and fined between 12 and 24 months".

• Finally, a typical action may destroy, alter or damage IT equipment (art. 263 CP) and data, information or systems. (art. 264.2 CP).

Both typical actions may constitute a crime against the market and consumers.

Finally, possible sentencing as considered in art. 255 of the CP is now being frequently applied as the use of hardware or software to defraud or misuse telecommunications networks owned by third parties is becoming more and more prevalent

Civil Code

1. Provisions.
   A) Civil Code
   B) Regulating Laws for Retail Trade
   C) Cheques and Exchange Law
   D) Interbank Operations Regulations
   E) Merged Text of the LGDCU

2. Proofs
   a) LEC
   b) Good Practices Code and Recommendations.

3. Directive 64/2007

Provisions relating to responsibility under Spanish law.

•Based on guilt and negligence (arts. 1101y ss del CC):

"Whoever, while going about his legal duty, incurs damages, negligence or debt shall be refunded the value of the damages, or whoever, in any way, fails to satisfy the tenor of the agreement".

•Good Faith, ex art. 1258 CC:

"Contracts are perfected by simple consent, and thereafter oblige not only fulfilment of the express pact, but also any consequence that, according to its nature, meet good faith, use and the law".

It is not appropriate to demand extra care from the card holder and yet to exonerate other parties implicated in the relationship deriving from the card contract.

- **Art. 1766 CC**, Once the obligations of the depositor have been established, he is obliged to keep the object and return it to the depositor, and is responsible for the safekeeping or loss thereof.

- **Art. 156 Exchange and Cheques Law**, states that damages resulting from a false or falsified cheque shall be at the cost of the payee unless the payer (E.F) acted with negligence.

- **Art. 46 Retail Law:**

When the value of a purchase has been paid using a credit card, when said card has not been directly presented or identified electronically, the holder may demand the immediate cancellation of the transaction.

The problem: the mechanism of this cancellation is not stipulated.

FINANCIAL PRODUCTS AND CONSUMER PRODUCTS

•Royal Decree 2507/2000, 1st September, expressly includes, "banking and financial services", inSub-section C. 1 annexe 1.

•The Law on Consumer and User Protection applies to financial institutions. (among others Sentence 123/98, Supreme Court Andalucía 9.03.1988).

•Under merged text of the LGDCU Financial services and products:

•Art. 88.2 from the merged text of the LGDCU. "The imposition of the onus of guilt is on the consumer in cases when it should be on the other party."

PROOF

•Regulated under the LEC

•European Code of Good Conduct and the Banco de España Best Practice Criteria.

LEC: General Principals of the Onus of Guilt:Art. 217

•It is held that there is an objective responsibility by the institution that creates and implants the system.

•Against that, the client who is supplied with a credit/debit card assumes the responsibility of its safekeeping. There is enormous disparity in the criteria of jurisprudence.

•"It must be remembered that proof of guilt of the card holder lies with the financial institution, who states that said limit may not be alleged" (Toledo 1.07.99).

•If neither of the two parties is guilty, the credit institution assumes the damages. In principal by application of the general rules of responsibility contained within the contract (e.g. in the supposed case of fraudulent withdrawals, the card holder shall only be responsible for the first 150€).

•In the case of negligence, either by the card holder or issuer/manager, the issuer shall accept arbitration on the question of responsibility. The only competent body shall be the courts of law.

Criteria of the European Code of Good Conduct 1987 on the question of electronic payments and the Criteria of Best Practice by the Banco de España

•Art. 15 CBC: "If the card holder denies that his card or PIN or any other password has been used for a transaction or alleges that the transaction was incorrect, the issuer must

demonstrate, using internal bank statements, that the operation was truly recorded and annotated in the holder's bank statements and was not affected by any type of error or deficiency. Proof in the first instance that the system operates correctly shall be the correct record of said transactions, whether they be prior to or post-transaction".

•On the principal of just and balanced distribution of risk. Originating from the circulation on the market of cards that act as methods of payment, as well as for other banking operations, without the need for intervention by bank employees.

•This has created the system and has established the safety mechanisms: objective responsibility of the institution. (Even though the issuer demonstrates that every possible measure has been put in place to avoid fraud).

Responsibility that is deemed objective after the card holder has reported a withdrawal and after the first 150€, that the holder shall be liable for. The issuer must prove incorrect use in general of the PIN etc. If the issuer establishes a system, they must be responsible for it.

Directive 2007/64/EC of the European Parliament on payment services in the interior market.

•**Guarantees a high level of protection thanks to material requirements of information and the definition of the rights and obligations of users and issuers of payment services.**

•Regulates:

•The execution of transfers

•Card payments

•Standing orders

•The issue or acquisition of payment instruments or money transfers.

•CONTENT IN RELATION TO CLIENTS:

Block 2. Transparency of the conditions and requirements for clear, concise and FREE information for all payment service providers. Stipulates:

•The conditions that should be communicated first

•The information that must be provided, upon demand by the user,Before a payment operation (time frame, commissions, costs);

•The information that must be supplied to the client who requests the payment after the transaction (operation reference and beneficiary, total value and costs and commissions, exchange rate applied etc);

•The information that the beneficiary must provide after receipt of the funds (references of the client who requested the payment, full value of the transfer, and costs and commissions, exchange rate applied etc);

Block 3. Basic harmonisation of the rights and obligations related to the provision and use of payment services. Stipulates:

•**Responsibility of the payment services provide**r in the case of non execution or defective execution of a payment: The latter shall be deemed objectively responsible, except in exceptional or unforeseen circumstances.

The burden of correct execution of the operation falls on the service provider.

Payment operations shall be considered authorised when the client has given his consent for its execution.

If no consent has been given, the operation shall be deemed unauthorised.

•**Responsibility of the payment services user:**

In the case of fraudulent use of a payment instrument the user's responsibility (excluding business use) shall be limited to 150€. The directive foresees two exceptions to the limitation of responsibility below, according to the actions of the user:

a) Fraudulent activity; or

b) Failure to comply, either deliberately or through grave negligence, with his obligations.

1 Recommendation 87/598/EEC, the Commission, 8th December, relating to an EU code of conduct and referring to electronic pages (DO L. 365, 24th December).
2 Published in the DO L. 317, 24 November 1988.
3 Published in the DO L. 208, 2 August 1997.
4 Published in the DO L. 275, 27 October 2000.
5 Published in the DO L. 319, 5 December 2007.
6 Published in the DO C 100 30 April 2009.

•Conditions for rectification: according to which the user may rectify an unauthorised or incorrect operation as long as he notifies, within 13 months from the date of the debt, even if there exists the possibility of agreeing on another term between both parties.

• The right to block an instrument of payment to the provider for reasons of card security;

The suspicion of unauthorised or fraudulent use of said card; or in the case of the card being associated with a line of credit, such as credit cards, there is a greater risk of the card holder not being able to meet his payment obligations.

3.2. Judicial regulation of electronic payment methods

We do not find, either within our own judicial system, or on a Community or international jurisdiction, extensive regulations pertaining to this matter. Some of the principal laws, directives and recommendations that form the basis of this analysis of electronic payment methods are:

A. EC Recommendations and Directives:

- Recommendation 87/598/EEC, of the Commission, 8 December, relating to a European code of conduct referring to electronic payments.

This code defines its objective in the following way: "The Code contains all the conditions that must be met so the new forms of payment can be developed in such a way as to be beneficial for all concerned and can offer:

- Security and convenience to the clients,

- More productivity and security to providers and issuers,
- An important market for European industry.

2. All those who apply or use card payment systems must respect the principals of loyalty laid down in the Code.

3. The technological evolution must respond to a European concept of electronic payment methods with the widest possible interoperability to avoid market fragmentation."

This Code of conduct attempts to guarantee security in the use of electronic payment methods not only for consumers and users but also for service providers and issuers.

As well as this, and something towards which there has been much work done, is for the interoperability of the systems on which these new payment forms are based. That is to say, in the establishment of systems that are operable market-wide.

- Recommendation 88/590/EEC, of the Commission, 17 November, relating to payment systems and in particular to the relationship between card holders and issuers

- Recommendation 97/489/EC of the Commission, 30 July, relating to transactions carried out through electronic payment instruments, in particular, the relationship between card holders and issuers

With this Recommendation, which updates the previous Recommendation, the Commission tries to favour the use of electronic systems by concentrating on payment systems as one of the essential elements to guarantee the complete working of the interior market.

In this way, it is attempting to contribute to the coming information society and, in particular, to electronic commerce by promoting client confidence in these instruments and the acceptance of the methods by retail trade.

- Directive 2000/46/EC of the European Parliament, 18th September, on access to the activities and operations of the electronic money institutions and the supervision of said institutions

This Directive, as stated by its 5th clause, is trying to establish guidelines that will permit a fuller use of the advantages deriving from the use of electronic money, and avoid the obstacles to technological innovation. The introduction of a neutral judicial framework from a technological point of view that harmonises the close supervision of electronic money institutions as far as is necessary to guarantee their responsible management, as well as their financial integrity in particular.

- **Directive 2007/64/EC European Parliament 13 November on payment services in the interior market by which Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC are modified and Directive 97/5/EC is supplanted**

7 Published in the BOE num. 15, 17th January and modified by Law 47/2002, 19th December, reforming the Retail Trade Laws.

8 La LOCM regulates, in Art. 46 card payments and refers to Art. 8 of EU Directive 97/7/EC which has been replaced by Art. 89, EC Directive 2007/64/EC European Parliament and Council 13th November on payment services in the interior market. Spanish legislation must place this Directive on the statute by 1st November 2009.

9 BOTANA GARCIA, Gema, states in Art. "Contracts with consumers and users" published in the newspaper "Diario" Law, Nº 6990 de16 Julio 2008.

10 Published in the BOE num. 281, 23rd November 2002.

The first clause of this directive states that it is fundamental for the establishment of an interior market, that Community frontiers disappear, in order to allow the free circulation of goods, people, services and capital. In order to achieve this, the correct operation of the single market payment services is vital. However, at present the lack of harmonisation in this respect is an impediment to said correct operation.

Clause 56 states that more detailed regulations must be established on the fraudulent use of cards, an aspect currently controlled under Directive 97/7/EC of the European Parliament 20 May 1997, relating to the protection of consumers in the question of distance contracts, and Directive 2002/65/EC. Said Directives should therefore be modified.

As a consequence, article 89 of the Directive proceeds to replace article 8 of 97/7/EC.

- The Decision of the European Economic and Social Committee

On the question "The fight against fraud and falsification in alternative payment methods", 23 October 2008.

B. National legislation

- Law 7/1996, 15th January, of Regulations in the Retail Trade, LOCM.

This regulation contains, in Chapter II, clause III, the first state-wide regulation on distance sales, which is in force for the regulation of business relationships. The Spanish Legislator had proceeded to modify arts. 38 to 48 which include precisely the aforementioned Chapter II, Clause III, with the aim of adding it to the statute book Directive 97/7/EC, in respect of distance contracts through Law 47/2002, 19th December.

- Law 44/2002, 22nd November, on Reform Measures to the Financial System.

This law dedicates Chapter IV to the "Push to use electronic techniques" and, particularly article 20 on the legal effects of electronic contracting and article 21 to electronic money.

- Royal Legislative Decree 1/2007, 16th November,

Which approves the text laid down in the General Law for the Defence of Consumers and Users and other complimentary laws, TRLGDCU.

Insofar as it affects us here, art. 106 of the TRLGDCU dedicated to card payments states:

"1. When the amount of a purchase has been charged fraudulently or improperly, using a payment card number, the cardholder and user may demand the immediate cancellation of the charge. In such a case, the corresponding debit and reimbursement entries in the accounts of the company and the cardholder and user shall be effected in the briefest possible time.

2. However, if the purchase was indeed made by the cardholder and user and the demand for a refund was not a result of having exercised the right of waiver or termination, he shall be obliged to compensate the company for damages incurred as a consequence of such a cancellation.

This precept stems from the card holder who discovers that his card has been used fraudulently or incorrectly in the contracting of a service. In this case, it foresees that corresponding records of debt and repayment in the card holder's and business's accounts are affected only for the briefest possible time.

When it is the consumer who acts dishonestly, art. 106.2 states that he shall be liable for the repayment to the affected business for all damages occasioned by the previously mentioned cancellation. The requirements of this exception are that the exact nature of the incorrect cancellation is established, as well as any damages that may arise to the business.

All these laws do not affect others that, without specific reference in the matter of electronic payments, may be applicable due to their treatment of related questions as may be the case with Law 34/2002, 11th July, on services within the information society and electronic commerce, LSSI, the Law on Electronic Signatures, LFE, decision that electronic payment methods are often, as we have seen, accompanied by electronic signatures or Common Law 15/1999, 13th December, Personal Data Protection, LOPD, applicable to all personal data treatments and which is used for the management of electronic payment methods.

Payment Services Law Project which aims to supplant our Judicial Statute for aforesaid Directive 2007/64/EC.

The specific objectives that this Law Project establishes in its Declaration of Motives are the following:

Firstly, to stimulate competition between national markets and ensure equal opportunities for competition. It allows for the creation of new payment institutions which, having fulfilled important demands and guarantees as to their correct operation, may represent an expansion of payment service providers.

11 Published in the BOE num. 287 30th November 2007.
12 published in the BOE of the General Courts 17th April 2009. Series A. Num. 25-1

Secondly, it will increase the transparency of the market as much for service providers as for users. To achieve this objective, it is vital to establish common regulations as a better system of offering judicial safety, nationally as well as internationally, as long as the conditions and applicable information requirements for payment services are uniform.

Thirdly, to establish a common system of rights and obligations for providers and users in relation to the provision and use of payment services. Without such regulation, the integration of a single payment market will be impossible.

PART 6

Annexe

Jurisprudence

The courts pass sentence on payment fraud

An analysis of legal resolutions

In this section we will take a look at different resolutions by judges and courts that refer to payment methods and their fraudulent use.

Firstly, it must be clear that the bank's responsibility is as a consequence of the risk created by the very activity being carried out; responsibility for professional risk, and quasi-objective responsibility (STS. 1st March 1994 SAP. Tenerife, 29th June 1993 and SAP, Madrid, 6th November 1992). A bank's due diligence is not that of a father, but that which corresponds to an expert in commerce who carries out his tasks of deposit and commission, which requires special care, particularly when we remember that the banks make a lot of their business in this way.

The Supreme Court states that those obligations of conservation and return are of an absolute character and only diminish under exceptional unforeseen and unavoidable circumstances. The sub-clause dealing with the care that must be demanded from a bank that carries out the function of depository and safekeeping of other people's money, declares that special care must be taken in these types of functions.

Therefore, when dealing with forms of payment, and even more so when the technological content is considered, it is clear that the care and responsibility taken by those who offer these systems to the user must be equal to its operation and security, and it is in this respect that many decisions have been handed down.

Bank cards: The courts demand greater care from the bank and building societies

Responsibility and burden of proof for theft and/or fraudulent use of bank cards

As was clear from the section referring to abusive clauses, the user, as was foreseen in the Recommendation and the European Directive on payment methods would be liable for losses deriving from unauthorised card use resulting from the use of a stolen card, to a maximum of 150€, once the theft or loss has been reported. Except in cases of fraudulent use by the holder, once the loss has been reported, the user would have no further liability.

However, the card issuer would be responsible even before notification, if they had not put in place every possible method for the holder to notify them as soon as possible of the theft.

SAP Alicante, Section 9, 30th March 2007: Cards have no specific legislation

"Credit card contracts are considered to be atypical contracts and as such have no specific legal regulation, and that is where the importance of the good will of both parties is important (art. 1255 of the CC), but we must not forget that as they are bank contracts, they are in the condition of adherent contracts whose clauses are imposed by a bank, who presents them to the client, who in turn signs them with a broad understanding but who enters into no negotiation, therefore the interpretation of the contract's contents should be in line with General Law 26/1984, for the Defence of Consumers and Users. On the other hand, this doctrine has come to mean the criteria of establishing that the card issuer bears the onus of proving grave fault on behalf of the user, as decided by the SAP of Asturias, 15th February 2005, and to which the SAP of Madrid makes express reference on 25th April 2006: Recommendation 87/598, 8th December 1987 of the European Union on the Code of Good Conduct in respect of electronic payments and 97/489 30th July 1997 that revises and updates it contemplate the responsibility of the card holder from the time of theft to the time of notification to the tune of 150€, except in cases where the holder has acted fraudulently or negligently (in which case, said limit shall not be applied),in the fulfilment of his obligations of use and adequate care of the electronic instrument, keeping the PIN secret, or failing to notify the issuer quickly of the theft, loss or falsification of the card (article 8.3 of the first and 6 of the second). The complaints service of the Banco de España, after 1991, began to state that in the case of non-compliance with Best Practices, then the limit would not be applied (reports relating to complaints 1334/91, 1514/91 y 25/92) and so, since then these have been incorporated into bank card contract".

The burden of proof is on the card issuer, as it is the issuer who has the best possible tracking methods for card movements available to him, the courts also recognise this responsibility of the financial institutions to protect the holder with every possible safeguard.

SAP Valencia, num. 200/2006, 17th May 2006: the risk must be assumed by the issuer

"(...) The consequential damages that may derive from such a risk must be assumed, in the first case, by the issuer, as they are the dominant party to the contract, the generators of the source of risk as it is they who issue the card in the first place and promote its widespread use; those who establish the rules and safety of card use which are stated in the contract and finally because they control and produce the

necessary technological means to ensure security. It is they also who have configured the point which interests us here, automatic telling machines, their location and their security measures. This assuming of the technical risk involved determines the responsibility of the banks as is recognised by the majority of jurisprudence (Sentence handed down from the Madrid Provincial Court, section eleven 7-12-2002; Asturias 18-3-2002, and Tarragona, section three,27-12-2004, this last in a supposed case very similar to that being judged here) unless the damages caused are attributed to the card holder (...)"

In the following paragraph, the same sentence apportions the rights and obligations of both parties-client and bank-which is clearly explicit: *"The card holder, as is established in the conditions of contract, has the contractual obligation to keep the PIN secret; not to write down the PIN on ant documentation he may take with him or that may accompany the card and to notify the bank immediately upon loss, theft or falsification of the card and the knowledge of any other party as to the card PIN. For its part, the bank is obliged to keep the PIN secret and to cancel any expired or reported cards, for among other reasons, the PIN will be known to a person other than the holder. The care taken in fulfilling these obligations cannot be of the same magnitude as that of the client-a consenting consumer-which, in accordance with article 1104 of the Civil Code, is that of a father, always tempered by the obligations imposed by and explicit in the contract, while that of the bank is that which can be demanded of a professional, given that it is the bank which prepares the system and has established, as is the case with automatic telling machines, the design and security measures. They are therefore in a better position to correct faults which may appear in said security, in accordance with the rules of onus of proof established in article 217of the Law of Civil Judgement, in which the bank must allege that the client displayed wilful negligence in the preservation of the card or the PIN (Handed down from the Toledo 1/7/1999, Malaga (section six) 23/7/2002and Madrid (section 12) 6/10/2004 , as far as is possible for the card holder to confirm that the movements on the card are fraudulent, that is to say not effected by him or with his authorisation, the burden of proof is apportioned by the judge. In consequence, for these unauthorised and illicit movements by a third party, only the card holder shall be held liable in the case of negligence or lack of due caution in his obligations of safekeeping and secrecy, in other cases the technical risk shall be assumed by the issuing institution who promotes the system (a criteria upheld in the decision handed down by Murcia Provincial Court –section 1- 29/9/2004).*

SAP Zaragoza, March 2006: problems and responsibility after the theft of a card

"The question (...) is in determining who should assume the risks deriving from fraudulent use of a stolen card, after a succession of movements-a withdrawal of 300€ at 18.58 on the 1-11-03, another for 300 € 1 minute later and then 3 minutes later a telephone card recharge of 100€- after one erroneous attempt to enter the PIN at 18.44(...

The judge concluded that if the criminal discovered the PIN with such ease, almost at the same time as opening the wallet, then it meant that the PIN must have been recorded in the wallet, which constitutes a grave breach of the obligation of safeguarding the PIN, a fact which, given the gravity of the negligence could only result in the card holder being liable for the full amount lost.

However, to infer from this presumption that the defendant had the PIN written down on some document within the wallet, basing this presumption on the speed with which the PIN was discovered and the operations carried out is adventurous to say the least, but what can be surmised is that nowadays, no-one has their PIN written down thus.

The impossibility of discovering the PIN so quickly is simple allegation from a biased perspective, upheld by affirmations made by bank documentation, which, at first glance, would appear to be confirmed by daily experience.

Finally, as negligence by the card holder cannot be proven, nor can the infallibility of the system as regards the discovery of PINs, the allegation that the full import of the losses be born by the card holder must be rejected."

Issue, retention and delivery of cards without prior consent by the card holder

We have already seen from the complaints service of the Banco de España that when the bank cannot accredit the request for a card from the client, the discretional issue of a card based on commercial criteria is contrary to Best Banking Practice. In this respect, the European Code of Best Banking Practice, with respect to card payment systems, and in the CBE num. 8/1990, establish the obligation of delivery and subsequent subscription by the client in the emission of payments through savings and current accounts.

In clause 8 of the code, it is established that a card issuer may not issue an unauthorised card to a client, except when this is to substitute another card.

By the same token, the sending of financial documents through unregistered mail, such as PINs and credit cards does not constitute documented reception of same by the recipient.

SAP Ciudad Real, 28th Novembe 2007: Non-delivery of contract

(...)It must be remembered that in the same way as realising the contract on the initiative of the issuer with no more requirements than those that are offered by a written document of which he has no knowledge and which cannot be proven even afterwards, risk shall be included and this provision is so clear that it cannot be ignored by an institution as notorious as the one in question. This risk, easy enough to contemplate hypothetically, shall be understood as assumed when irregular or fraudulent use occurs, as appears to be the

case here. Although no initiative has been taken to record the risk and so there has been a drift towards responsibility for the amount demanded. In this respect, looking at the charge that the claimant has incurred, and from where the accused has proven that no order was signed directly and personally by him, something he could not have done given his circumstances, (deafness and illiteracy) it was also possible to accredit the identity of the person who used the card, at least as far as acquisition of the video is concerned, and independently of the fact that a price was paid and not included in the petition that is the subject of this case, as well as the identity of the various statements taken from different bank branches who video such operations. (a form of proof which has been neglected in the case). Therefore the case is one of, at the very least, having reduced the very many possibilities by which the credit card could have been used (members of the family or people known to the accused, who is retired and living in a residency, all of those who could know the requirements needed on the form) and also counting on certain indications that would permit the acceptance of the accusation that – are not the same as having charged the previous receipts given the aforementioned personal circumstances – on the contrary, admitting the aforesaid, it is not viable.(...)"

Incorporation of abusive clauses within a contract: common practice with cards

The financial institutions, in order to avoid responsibility in the case of unauthorised card use include abusive clauses in contracts such as: period of 24 hours to notify of loss, theft or falsification and limit the holder's liability to 150€. Several decisions have considered these clauses to be abusive, as notification is not a question of time but of the realisation that the card is missing. With reference to the Civil Code, art. 1.255, states that "the contracting party may establish pacts, clauses and conditions they consider to be convenient, as long as these are not contrary to existing laws, morals or public order", or the general condition that a contract must fulfil, which prevents the existence of abusive clauses, such as those established for fraudulent card use.

SAP, Madrid, Section 21, num. 446/2007, 18th July 2007: responsibility cannot be limited

The claimant was a holder of a card issued by Caja España, linked to a current account in his name. The contract is supplied herewith for the card dated 19-2-2001, (...). Clause 5 on "Limitation of responsibility says: the holder shall assume responsibilities deriving from the fraudulent use by third parties before notification foreseen in sub-section b).3 clause 4. This responsibility shall be limited to a maximum of 25.000 Ptas. (150,25 €), as long as the loss or theft is reported within 24 hours of its occurrence and there has been no fraudulence or grave negligence on the part of the holder. Notwithstanding, grave negligence shall be understood as such a situation as the PIN shall be in some way connected to the card, so that the thief gains knowledge of it".

The court upholds the sentence in respect of the declaration that the 24 hour reporting period was not respected, as is established in clause 5 of the aforementioned credit card contract. This resolution stems from the fact that it is not contrary to the balance of responsibility of and between both parties contained in clause 5. But it argues that the short time period allowed to report the theft does break the balance, in such a way as that it shall only be fulfilled under exceptional circumstances, placing disproportionate responsibility on the card holder. This evaluation is fully concurred with by the court and upheld by the resolution that mentions the Judgement "a quo", Sentence of Madrid AP, Section 8, 28-11-2003, which also adds that "the imbalance in the rights of the consumer insofar as it concerns the court, not individually negotiated, as said clause was laid down previously and could not be influenced by it. The time scale of 24 hours makes it extremely difficult to indemnify and offers a benefit to the injured party (issuer) who shall be exempt from indemnifying the card holder except on occasions when this time scale is fulfilled". It is therefore deemed abusive "for not holding fast to the demands of good faith, being disproportionate, causing notable prejudice to the consumer and implying an imbalance in the obligations of the parties with respect to (...)", in application of art. 10.1 c), 3 y art. 10 bis of the LGDCU , according to the decision given by the First Amendment to the Law on General Contract Conditions .

Bank transfers: errors and failure to meet time scales, the most common causes in the courts

The contract for a current account is an atypical contract through which a telling service is offered whose results are noted in the form of an account by the current account system. The bank realises payments of a wide variety, according to the instructions of the client and the availability of funds, and in the case of a lack of precise instructions, acts in accordance with common law and good banking practices, loyalty and profit for the client.

Within the bank services offered in a current account are the services of bank transfers (multilateral operation where several subjects may intervene-the originator, beneficiary and credit institution). The relationship established between the originator and the financial institution is under a contract of commission for which legal regulations shall be applied insofar as the determination of due care and responsibility is concerned (SAP, Castellón 24th April 1997).

In respect of the question of the onus of due care that befalls the bank, it is subject to jurisprudence, which affirms that it is not that of a good father but that of an expert businessman who normally carries out the functions of deposit and commission (STS, 22nd September 2005; SSTS, 15th July 1988 and 9th February 1998). Therefore, given that it is the bank who given that it is the bank which prepares the system and has access to the necessary personnel, material, design and security, and is therefore in a stronger position to correct the faults, it follows that the onus is on the bank to prove negligence by the client.

SAP, Alicante, Section 9, num. 136/2007, 18th April: there are also problems in money wires

"(...) The behaviour of the Foreign Exchange Company España SA, trading under the commercial name of Western Union, was not blessed with due care and good practice as demanded of these institutions dedicated to a professional service of money wiring. Given that a debt of loyalty, information and prevention is to be expected as a consequence of the professional image it boasts and of the relationship of confidence which the client feels before such an institution, a model of businesslike professionalism, it should be held responsible for all damages resulting from negligence in the course of its duty.

STS 10th July 2003: negligence by banks and building societies when carrying out a money transfer

"It is therefore a measure that meets an objective and abstract criteria. Due diligence is demanded according to circumstances that, within social life can be demanded in a particular situation from a reasonable person who is qualified to judge the activity. According to this criteria (the man on the Croydon omnibus) the question of whether the agent acted with all due care, attention and perseverance, with the necessary reflection and sacrifice of time, must be resolved. Furthermore, the individuality of the agent is not therefore decisive, but rather the circumstances that determine the necessary degree of due diligence."

Transfers are carried out in accordance with the regulations of the National System for Electronic Compensation, according to the instructions of the client. The transfer order, in accordance with the contract stipulations, obliges the bank to not only carry out the transfer, but to ensure its satisfactory conclusion.

Therefore, said operation shall be that which determines the level of due diligence employed by the institution in each particular case (SAP, Vizcaya, 18th January 2000. Establishes the bank's negligence when it carried out a transfer order after it had been refused by the client.). From a procedural point of view, the aforementioned due diligence implies that even in the case that the complaint is laid exclusively at the door of the institution.

Finally, and as an example of negligence by the institution in relation to the correct execution of an order, the following can be cited: the execution of a transfer order without establishing the identification of the client (STS 15th July 1988, RJ 1988/5717); realisation of a transfer to a different account than that of the recipient (STS 14th November 1987, RJ 1987/9987); the repetition of the same transfer (SAP Valencia, Section 8, 15th June 1999); realisation of a transfer whose order had been given by telephone in favour of a person other than the title holder of the account, without confirming the authenticity of the signature on the written instruction (SAP Malaga, Section 5, 14th February 2001)

Setting up of unauthorised standing orders

This a modern practice that the banks have implanted supposedly to allow greater agility, but in reality to their own benefit. It consists of the indiscriminate ordering of payments, which it is not in the bank's power to do, and is the establishment of a standing order on an account with the correct account number. In these cases the bank has to inform the client of the order in the shortest possible time so that he may decide to pay it or not

SAP Seville, Section 2, num. 254/2005, 6th June 2005: the bank must not pay payment requests that have not been authorised by the client

"The statements of bank movements reveal that Banco Popular and Dª Carmela are joined in a bank contract for the opening of a current account, and, although the document itself has not been presented at this hearing, it is obvious that there can be no clause stating that the bank may honour of its own volition standing orders against the client's account or receipts not issued in her name or unauthorised payments.

On the standing order for telephone charges, on page 7, it clearly indicates the number to which the standing order refers and only this may be paid by Banco Popular from Sra. Carmela's account.

The payments made in the account correspond to num. NUM000 (and referenced under quantity NUM001) are incorrect as the standing order only includes invoices relating to telephone num NUM002; the bank has failed to comply with its obligation of diligently safekeeping the money deposited through the current account contract between 1997 and 2002, and has paid invoices for which it had no authorisation.

As there is no correspondence between the order to pay Telefonica invoices and payments made from the current account, the bank, which was not authorised to make payments from the account telephone bills for NUM003, must respond for irregular or defective fulfilment of its obligations, constituting a contractual blame under art. 1101 of the Civil Code."

Cheques: the most widely reported falsifications

STS, Penal Court 2, num. 1195/2005, 9th October 2005

Damages resulting from payments by a false or falsified cheque shall be the liability of the issuer and not the recipient, except in case where the recipient has been grossly negligible in the safekeeping of the chequebook, or if he had proceeded with malice. Falsification of a cheque in order to commit fraud and its subsequent use by the author of the falsification to commit fraud, must be sanctioned as a crime between serious fraud and falsification of a mercantile document.

SAP Madrid, Section 21, num. 463/2006, 27 October 2006

Damages resulting from payments by a false or falsified cheque shall be the liability of the issuer and not the recipient, except in case where the recipient has been grossly negligible in the safekeeping of the chequebook, or if he had proceeded with malice, therefore there exists a certain objective responsibility ex lege by the bank, by which only cheques issued by the holder are authorised.

STS Civil Court 1, 18th July 1994

"Art. 156 of the cheques and exchange laws(on which the action is based), typifies a specific supposition of responsibility by contractual guilt, the express motive must be ignored, because if indemnity responsibility that, in accordance with the first instance of the cited precept corresponds to the receiving bank for damages incurred on honouring a false cheque, this may be totally excluded or eliminated when the account holder (the issuer) has been negligent in the custody of the chequebook or has proceeded with malice (second and third instances of the same precept), it is indubitable that, when negligence exists on the part of the receiving bank, there is also an evident guilty conduct by the issuer of the cheque, whose guilty concurrence, as is the case in all cases of responsibility by contractual or extracontractual guilt. Sentenced in this court 18th October 1982, 22nd April 1987, 7th June 1991, among others), is indubitable, that in said supposition the courts must moderate the responsibility of the agent and reduce his duty in proportion to the indemnity, sharing the damages with the injured party.

When it is not possible to present the cheque, protest or make an equivalent declaration within the stipulated time because of force major, said stipulated time shall be deemed prolonged."

Phishing: a new form of fraud that already has recourse in the courts

Phishing is a crime in which the perpetrators usurp access codes to bank accounts belonging to the victim with the aim of stealing money. This type of delinquency has proliferated exponentially in recent years. In addition, organised gangs use ever more technical, modern and complex methods that make their detection and avoidance even more difficult.

In the face of this there is another, equally important problem for users of financial institutions: the exoneration of responsibility clauses that the institutions include in their contracts (adhesion contracts). This means that in the case of a client falling victim to this type of fraud, he will have to assume the full economic cost.

A case won by ADICAE

"(...) As stated by the Madrid SAP, Section 13, 11th February 2005 the referred clauses displace the bank's responsibility to the client who has taken no part in the damages caused, in direct infringement of the facts contemplated in clause 14 of the First Amendment to the General Law for the Defence of Consumers and Users insofar as the limitations imposed on the rights of the consumer." (Judge nº 2, Castellón, num. 126/2008, 25th June 2008. Legal Finding. 6, favourable sentence for the consumer obtained by ADICAE)

In this respect this finding from the Law Courts in Castellon is a great step forward and important achievement for ADICAE in the defence and protection of consumers' and users' rights in on-line banking services. The resolution found in favour of the clients, indicating that the bank has the obligation to supply its clients with clear and precise information on the security recommendations that should be employed when accessing an on-line banking service.

In General Stipulation IV, of said contract it states that "Building Society B" is exonerated from all responsibility owing to deficiencies and security faults in the communications networks, such as a virus or owing to the use of a deficient or poorly configured navigator. Neither will "Building Society B." be liable for damages caused by the illegitimate insinuation of third parties into the system.

Finding 6: (...) it is not a given to impose upon the consumer the indiscriminate rejection of the right to complain to the bank who supplied him with the necessary technical means for better or more convenient services, in those cases where, being unworthy of consideration as a one off case or of force major they are effectively non-attributable to the bank even when damages occur.

They did not foresee or adequately inform the client

Related to everything that has been exhibited, the conclusion arrived at by the Complaints Service of the Banco de España must be made public in a report dated 23rd November 2006 ... before the complaint by the present plaintiffs for the same reasons that have hitherto been subject of a civil case. As the Banco de España states in the second legal consideration, and having revised the documentation supplied with the file, among which is the on-line banking services contract dated 14th November 2005, identified as 1486296, this doesn't mean that the building society supplied the client with the necessary warnings to avoid fraud during electronic commerce before the controversial transactions took place.

And although it may be true that this service is not competent to determine the consequences of its pacts, clauses and conditions established in respect of relationships controlled by private right regulations as the conclusion of discrepancies that may be produced in mercantile relationships between parties is the exclusive competence of the law courts, it is however, one more piece of information to bear in mind in civil jurisdiction (where there have now been questions raised as to the contractual relationships between parties) the fact that said organisation, after examining the documentation presented by both sides, has not been able to ascertain whether the bank did in fact offer its client all the relevant clear and concise information on security recommendations that should be employed each time the client accessed the online bank .

Therefore, the Complaints Service of the Banco de España has left the reach of its decision perfectly clear, and without doubt, what has been informed does not oblige the parties of this civil process, but this judge feels that the authorised opinion of the experts on the panel of the aforementioned service should be taken into account in respect of "Building Society B" as it refers to the information and security recommendations given to its clients in the online bank.