INTERNATIONAL PROJECT ADICAE

Measures aimed to the creation of a European technical catalogue against the fraud in means of payment

Introduction to and discussion of the technical proposals against the fraud by ADICAE

Comparative of the countrie's legislation, Minutes Seminar Madrid, Juridic Comparative Annex

Organises:

ADICAE
Association of Users Banks, Savings Banks and Insurances

With the collaboration of:

Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission, DG Justice, Freedom and Security

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 200107

INDEX

INTRODUCTION

Manuel Pardos:

Chairman of ADICAE, FSCG member (Financial Services Consumer Group) and FPEG member (Fraud Prevention European Group) of the Commisión European, member of the Consumers and Users Council of Spain (CCU).

Both by volume and value, transactions made through electronic payment instruments account for a growing proportion of payments made in the EU and beyond. The trend indicates that, in the coming years, electronic payment methods will become easier due to technological advances and it is expected that their use will become more widespread among consumers.

The possibility of using these payment methods practically all over the world requires that they be effective, easy to use, widely accepted, reliable and available to most of the population of Europe. Furthermore, it is essential that widely accessible payment instruments have the highest possible security measures against fraud, both before and after a crime is committed. This engenders consumer confidence in these non-cash alternative methods of payment, and therefore their success and expansion.

The increase of payment fraud in recent years, which is linked to more widespread use, is a concern. The expansion and transnational nature of fraud, therefore, requires cooperation and dialogue between all countries and protagonists (banks, security companies, card issuers, consumers, judges, police forces, etc) in order to create a coherent prevention strategy at European level. To date, the measures taken by member states, despite being effective, have not been sufficient to counteract the threat of fraud in the present and in the near future.

ADICAE has therefore developed a project entitled "Establishing a European technical fraud dossier available to judicial and police authorities based on a network of information alerts provided by banks and citizens" with the support of the European Commission and in which other European consumer associations participate. This project's general conclusion highlighted the shortcomings of policies and strategies of cooperation between European Union countries to date. It is therefore necessary to adopt several measures, which, following various presentations and debates, are analysed in this publication. Measures that particularly stand out include the elimination of bad practice and unfair terms in payment method contracts, in which banks exempt themselves from any liability in the event of fraud; the implementation of a series of measures such as fostering information exchanges and cooperation between public and private bodies; the harmonising of national laws in terms of prevention and suppression; the creation of a database coordinated by Europol to be used by different competent bodies relating to the investigation of fraud in each European Union country; and cooperation between European consumer associations, police forces, judiciaries, companies, banks, etc, to carry out widespread information campaigns to improve the awareness of users and educate them in the use of payment methods.

These and other findings and proposals that were presented at the European Symposium, "The economic crisis and payment fraud in Spain and the European Union", have been included in this publication, which ADICAE hopes will provide an impetus to the adoption of measures and solutions to curb the phenomenon of payment fraud, which is of such concern to consumers.

PART 1

Creation of a european technical catalogue against the fraud

Project introduction

PRESENTATION OF THE EUROPEAN PROJECT

Due to the alarming increase in payment fraud faced by consumers and the other than hopeful prospects for the future, ADICAE undertook this European project entitled "Establishing a European technical fraud dossier available to judicial and police authorities based on a network of information alerts provided by banks and citizens" with the support of the European Commission and the participation of other European consumer associations.

PROJECT OBJECTIVES

Non-cash payment fraud in the EU has an impact on hundreds of thousands of users and the security of the system itself. Current figures and the increasing growth expected in the coming years make the adoption of measures in all countries necessary, especially in those countries that have recently joined the EU and future candidates for accession. Fraud resulting from the gradual expansion of electronic payment, investment and a growth in tourism (with increased mobility of EU citizens) in these countries represents a particular risk.

The objectives of the project were:

- The cooperation of users and victims in reducing payment fraud in partner countries.
- Increasing the awareness of organisations that represent users in terms of type, mechanisms of fraud and protection.
- Facilitating the exchange of information regarding transnational fraud, enhancing coordination and cooperation between the various protagonists at European level, and coordinating measures taken in response that are common to all EU countries, thus mitigating risk by ensuring crisis management and a faster and more consistent response in the event of cross-border crime.
- Promoting cooperation with public bodies responsible for combating fraud, which helps to prevent or reduce risk.

PARTICIPATING COUNTRIES

ADICAE

Asociación de Usuarios de Bancos,
Cajas y Seguros de España

Slovenia: "Asociación (MIPOR)""

Slovakia : "Asociación nacional eslovaca de consumidores (ASC)""

Italy: "Associazione (FEDERCONSUMATORI)"

Lithuania : "Lithuanian National Consumer Federation (LNCF)"

Czech Republic : "Sdružení českých spotřebitelů (SČS)"

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

PROJECT ACTIVITIES

The following materials/activities were prepared/organised to disseminate the findings and conclusions drawn after months of study and research to ensure that the information reached judicial authorities, the Police and consumers:

- Technical dossier.
- Website with a fraud alert network.
- A study on the impact of fraud on consumers .
- European Symposium.

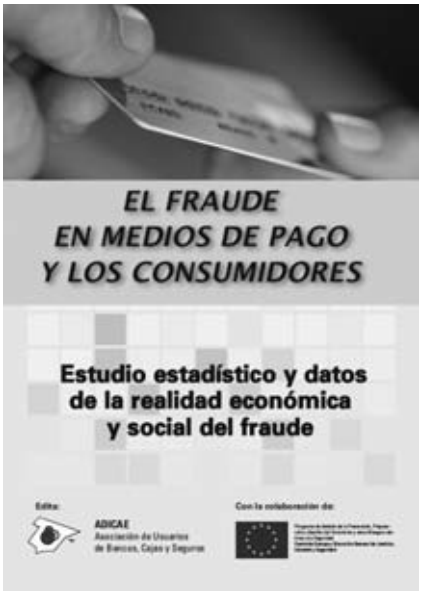
Technical dossier: a tool for training and debate

This publication, the cornerstone of other project activities and publications, aims to raise awareness and alert the judicial authorities and the Police of the risks to users and, in turn, inform advanced users of how payment methods work technically and how criminals operate by applying new technology to defraud. The aim is for the authorities to take measures and provide solutions depending on their competences and for advanced users to fully find out about fraud and how to avoid it.

Furthermore, an additional aim is to provide companies in the payment sector, consumer authorities and banks, etc. with a tool to exchange viewpoints and analyse the current situation of payment users in order to enable them to carry out their work more effectively.

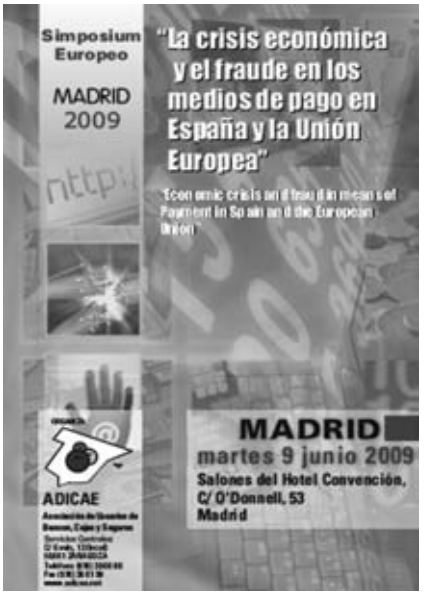
Survey on the impact of fraud on consumers

One of the ADICAE's concerns was to record the impact of payment fraud on households, and how it influences users when using their cards, electronic banking, etc. We conducted a comprehensive survey by obtaining information from recent studies carried out by organisations, institutions and companies specialising in payment fraud and also from a survey conducted by ADICAE, both in person and through the Internet, since it was available to anyone visiting the site. The information and results are intended to explain the situation currently experienced by consumers, as well as suggesting reasonable and feasible solutions for all those involved in payment methods.

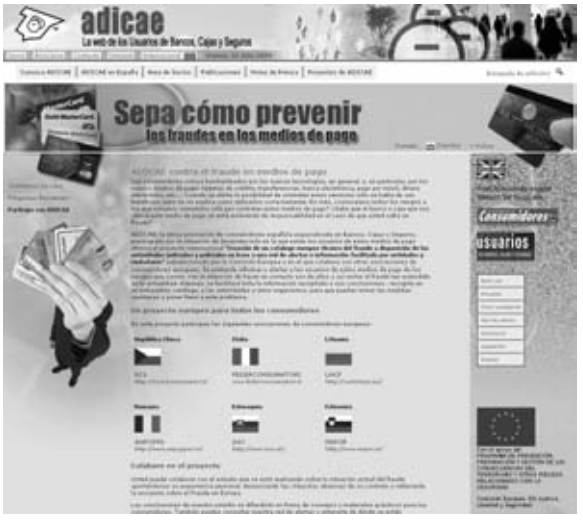


European Symposium: sharing information on current problems and proposals for future solutions

The climax of the project, in its final month, was the organisation of a European Symposium, "The economic crisis and payment fraud in Spain and the European Union," in Madrid on June 9th, whose contents are reproduced in this publication. The symposium was attended by speakers and figures from the field of consumer affairs in general and experts in payment security in particular. The aim was to bring together all protagonists so that they could offer their views regarding payment methods in the face of fraud and their proposals for solving the problem.



Website: Alert network (information and training)



ADICAE's website, www.adicae.net presents the project to all of its visitors and provides them with the opportunity to find out about the many types of fraud that exist, a dictionary with the most common terms, advice on how to avoid fraud and a survey that collected the opinions of payment users faced with fraud. All of this content has been a resounding success and we hope that the website continues to receive a large number of visits.

Another important part of the website is the alert network that ADICAE updates regularly to warn users of the latest types of fraud. This system is not intended to be active for the duration of the project, but to update and amplify all kinds of information relating to this issue on a daily basis.

PART 2

European countrie's legislation

Legislative framework and particularities

ROMANÍA

1. General legislative framework

Consumers' protection in Constitution

The fundamental Romanian law does not contain special stipulations regarding customer protection. Though there are some constitutional disposals that refer to the protection offered to the citizens as customers.

For example, art no. 135 line 2 letter a) from the Constitution adopted in 1991 and reviewed in 2003 stipulates that the State must secure "a free trade, protection of fair competition, provision of a favourable framework in order to stimulate and capitalize every factor of production". This disposition mainly refers to encouraging trading and competition without mentioning about protecting the customer. However it is well known the coexistence between free trading, fair competition and protection of customer's rights, who are direct beneficiaries of production activities.

Art. 17 also stipulates "The State shall be bound to take measures of economic development and social protection, of a nature to ensure a decent living standard for its citizens". It is obvious that this kind of measures involve protection of social and economic interests of the citizen. /A decent living standard can be assured only by defending their interests as consumers.

An important disposal mentioned in art. 21 is the one regarding the citizens viewed as consumers: "Every person is entitled to bring cases before the courts for the defense of his legitimate rights, liberties and interests". The present statement guarantees free access to justice which is a fundamental right and an imperative condition of juridical efficiency.

The essential principals that fundaments the most important customer rights are the ones mentioned in Chapter II entitled "Fundamental rights and freedoms". Art. 22 guarantee the right to life, to physical and mental integrity. These stipulations need to be corroborated with art 5 from the Regulation of Consumption which mentions The State's obligation to assure "the customer's protection against the risk of achieving a product or a service that may harm their life, health, security or that may affect their legitimate rights and interests". Other principles mentioned in the same chapter that may be connected with the customer's rights are: the right to defense, the right to information, the right to protection of health, the right to a healthy environment, the right to association, the right to private property, the right of petition. All these fundamental citizen rights are also found in the specific legislation regarding the customer's protection. The exercise of these constitutional rights can only be limited by law, in special conditions of necessity and adequacy.

All these fundamental prerogatives mentioned in the Romanian Constitution are highly connected with the customer's rights and benefit of an efficient application if they are internationally recognized (conventions, treaties, international agreements). A priority to any state is the recognition, guaranteeing and defending the fundamental rights and freedoms of the citizen (including the ones regarding the protection of the customer).

As a conclusion, the legislation regarding the protection of customers is not in contradiction with the constitutional right to free access to justice, the right to defence or indiscrimination although it has an obvious protective character in favor of consumers.

Regulation of means of payment in the Civil Code. The contracts.

The special legal disposals which regulate the protection of customers are completed with the common right, especially with the dispositions mentioned in the Civil Code. Inspired from the French Civil Code, the Romanian one contains in Book III, Title III disposals that regulate the contracts. Among these, there are stipulations that refer to the necessary and essential conditions to validate a convention. Non – compliance with these conditions conducts to the nullity of the convention.

In order to validate a contract, (also for the contracts where one part is a consumer), the assent must fulfill certain conditions: to come from a person with judgment; to be expressed with the intention of producing juridical effects; to be exteriorized and to be valid (not to be altered by any vice of consent).

Another type of vice of consent is the lesion, although the Civil Code does only give the minors the possibility to invoke this kind of vice. The lesion consists in the major disproportion between the prestations of the parties. The abusive clauses may create an economic lack of balance in the consumer's disadvantage.

The consumer must express a free and unviced consent when closing a contract, although he is situated in most cases in a position of economic inferiority reported to the professionals.

In case his will was altered by any vice of consent, the illegal contract must be canceled in order to protect the consumer's interests. The sanction in this case is the total nullity of the contract that in some situations may be in the detriment of the customer.

Plus, it is very hard to prove the vice of consent by the

party who claims it. Although the tendency of the juridical practice is to encourage and to facilitate the mission of the plaintiff, the probation task is not turned down in litigations between professionals and consumers. The professional's dishonesty is not presumed, the consumer has to prove it.

For all these reasons, invaliding the abusive clauses is preferred over the vices of consent, less used in the matter of customer protection.

2. Applicable law – particularities

The professionals, regarding the field of activity, must ensure complete, correct and precise information about the essential characteristics of the products and services provided to consumers. This obligation to informing the partners must be reinforced in the financial area.

n the banking area was adopted Law no. 289/2004 regarding the judicial regime of credit contracts for personal needs, designed for individuals. This law establishes the terms and conditions for closing a credit contract for personal needs, and contains several clauses in order to protect the consumers.

Another regulation designed to protect the consumer in the financial area is OG 85/2004 regarding the consumers' protection when closing and executing contracts by correspondence. These legal stipulations refer to the conditions of informing the consumers in the financial contracts regarding the banking services, credit cards, insurances, private pensions, financial investments.

These legal norms together with the ones in common law, defend the consumers' interests in the financial area and ensure enough protection to the "weak" part of the financial contracts.

Among the consumers' rights, the most important ones regard the following:

- The right to information: the services provider has the obligation to inform the customer in time, correctly and completely over the essential elements of the contract. The provider has the obligation to prove the fulfilling of this task, any contrary clause being considered an abusive one.

- The right to unilateral denounce the contract, with mentioning the terms and conditions the consumer may exercise it.

In contradiction with the legal specific regulation in matter of credit contracts, the following situations were met in practice:

- By analyzing several contracts, the result was that not all bank units explained clearly certain terms like mortgage, franchise etc., in order to be understood by the consumers.

- There is no clear specification about the penalty percentages for a late payment of a rate, the interest, the possibility of the consumer to unilaterally close a contract with 30 days notice.

- The lack of a clear elaboration of the contracts.

- The lack of information regarding deadly period, means of execution, suspension or stopping the service: terms, notifications, deposit conditions, insurance conditions.

Other applicable laws:

■ Law 365/2002 modified by law 121/2006 regarding electronic commerceGovernment decision no. 1308/2002 for approving the methodological norms regarding e-commerce.

■ Law no. 677/2001 for persons' protection regarding using their personal data.

■ Order no. 52/2002 regarding the approval of minimum security requests for using personal data.

■ Law no. 455/2001 regarding electronic signature.

■ Government decision no. 7/2004 regarding the juridical protection of services based on conditioned access.

■ Regulation 4/2000 of National Bank of Romania regarding distance payment means.

CZECH REPUBLIC

1. General legislative framework

Harmonization of the Czech legal framework had been completed with relevant acquis up to 1 May 2004, the date of accession of the CR to EU.

■ Criminal Code No. 140/1961 Coll.

■ Civil Code No. 40/1964 Coll.

■ Commercial Code No. 13/1991Coll.

■ Act. No. 254/2004 Coll., on restriction of payments in cash.

■ Act No. 253/2008 Coll., on some measures against legalization of profits from criminal activities and against funding of terorism.

■ Act No 253/2002 Coll. on transfers of finances, electronic finances and payment systems (law on payment systems).

■ Decree of the Czech National Bank, on the way of performance of payments among banks, acounting on bank accounts and technical procedures of banks for corrective accounting

2. Applicable law – particularities

Follows a review of some of legal arrangements against frtauds in the area of non cash payments in the CR, including relevant EU acts transposed into the Czech regulations

.■ 97/489/EC: Commission Recommendation, transactions by e-pyament

■ 87/598/EEC: Commission Recommendation, European Code of Conduct on e-pyament

■ 97/7/EC: Directive of the EP and C on the protection of consumers, distance contracts

■ 2001/413/EC: Council Framework Decision on combating fraud and counterfeiting of non-cash means of payment

■ 2000/31/EC: Council Framework Decision on combating fraud and counterfeiting of non-cash means of payment.

■ 2007/64/EC: Directive of the EP and C on the payment services

SLOVAK REPUBLIC

1. General legislative framework

Consumers' protection in Constitution

Even the Slovak Constitution was established quite some years ago, in 2002 – The Slovak Republic was established after splitting of former Czechoslovakia Jan 1, 2003 – the consumers are not mentioned in it. Constitution does not recognize the category " Consumer".

Constitution of the Slovak Republic

- article 26 , paragraph 1,4,5 – right to information
- art. 36, par. c and art. 40 – right to health-protectio
- art. 46 – right to independent law-court

Regulation of means of payment in the Civil Code

The Slovak Civil Code is based in former Czechoslovakian Civil Code 40/1964 which has many, many novels and amendments adopted during the last 44 years.....

■ Civil norm (civil code) applicable to contracts in general

- Act # 40/1964 plus its novels
- Contracts generally – par 43-51
- Consumer contracts – 52 - 60
- Contract of purchase – par. 588 – 627
- Deed of gift - par. 628 – 630
- Contract of work - par. 631 – 651
- Contract for repairment and adjustment par. 652 – 656
- Loan contract - par. 657 – 662
- Rental contract - par. 663 – 723
- Collection contract - par. 724 – 741
- Accommodation contract par. 754 – 759
- Transportation contract par. 760 – 773
- Commission contract par. 774 – 777
- Insurance contract - par. 788 - 828

■ Consumption norm (code of consumption or similar norms)

- Consumer Act 250/2007 effective from July 1, 2007
- Consumer rights par. 3
- Information duties par. 11 – 18

2. Applicable law – particularities

As for direct cash payments they were efforts since 1990's to fight through Tax-legislation against money-laundering by the cash-limits for payments made outside of banking system but it was not effective and direct cash-payments of even high amounts are very common

Credit cards

The misuse of credit-card is regulated in the System of payment-Act No 510/2002 effective Aug 31, 2002, art. 25 – duties and claims of consumer vs. bank/card issuer in cases of card-misuse..

Criminal Code No 300/2005, art. 219 – Forgery and unauthorized use of an electronical payment mean and other payment card - the basic punishment is 1-5 Years of imprisonment and 5-12 Years in special cases – big damage, as a member of dangerous organized group.

Even the rules can be considered as clear and sufficient in practice there are many problems in case a card or idenification data of a card were misused a consumer was damaged by ilegal withdrawal of cash from his/her money-account. In most cases banks/card issuers are not willing to accept consumer's point of view or arguments and usually declare that the consumer caused the problem and on the side of card-issuer no mistake occured - mainly in case when the author of the fraud is unknown, which is very common.

Transfers

The System of payment-Act No 510/2002 effective Aug 31, 2002, arts. 3-11 for inland transfers and arts.12-20 for international transfers. No specific provisions for Consumers were identified.

Cheques

No specific provisions with reference to consumers were identified.

Payments on line

Payments on line tied to information technologies – computers and internet systems.

The System of payment-Act No 510/2002 effective Aug 31, 2002, arts. 21 – 24.

SLOVENIA

1. General legislative framework

Consumers' protection in Constitution

Consumer protection is not mentioned in the Constitution. A special Law on Consumer Protection is the centrepiece of consumer protection legislation.

Regulation of means of payment in the Civil Code.

The main body of law in this field is not the Civil Code, but the Code of Obligations. Further specifications are the Law on Consumer Protection and the Law on Means of Payment. The mentioned laws were extracted from cases on card theft and phishing which we could find until now.

- Code of Obligations
  - Art. 5: Principle of conscientiousness in fulfilling contractual obligations
  - Art. 6: Principle of carefulness
  - Art. 86-88: Nullity of contractual conditions
  - Art. 121-122: General terms and conditions and their nullity

- Law on Consumer Protection
  - Art. 23-24: Prohibition of unfair contract terms
  - Art. 45: Dispatchment of undesired advertising messages

- Law on Means of Payment
  - Art 9.: Obligatory content of general terms and conditions
  - Art. 13: Obligatory content of payment order (identification,....)
  - Art.24: Obligation of compensation in payment transactions, resolution of disputes

- Law on electronic communication
  - Art. 109: dispatchment of undesired advertising messages

- Law on Banking
  - Art. 230: Dispute resolution among banks and consumers

- Law on Protection of personal data → Penal Code
  - Art 154: Abuse of personal data
  - Art 225: unauthorized entry into an information system
  - Art. 242: invasion into an information system
  - Art 309: Production and acquiring of tools intended for penal acts

2. Applicable law – particularities

Cheques

Cheques are regulated by the Law on Checks. However, today, the use of cheques is negligible in Slovenia. They are not an obligatory means of payment anymore. Some banks don't offer them anymore, while the consumers can obtain them at others through a special application. That is why we propose to leave this field out in Slovenia and concentrate on more important ones.

Country	Penal Legislation on Fraud
Czech Republic	Yes (Penal Code , 140/1961)
Italy	Penal Code: Section 491: Counterfeit of electronic documents; ; Section 635-bis: Damages to computer networks and lelecomunications; Section 615: Virus and Malware Difussion; Sección 392: Damages to property (included electronic goods); Section 494: Personality Theft
Lithuania	Yes
Romania	Yes
Slovenia	Penal Code: Art 154 (Undue use of personal data uso); Art 225: Non-authorised access to computer systems; Art. 242: Invassion to information systems; Art 309: Production and acquisition of tools for illegal acts
Slovak Republic	Penal Code nº300/2005, § 219 – Counterfeit and non-authorised use of electronic means of payment and payment cards

BULGARIA

1. General legislative framework

Consumers' protection in Constitution

Art. 19 of the Constitution, Market free economy, based on a free initiative, where the law guarantees equal conditions for economic activity to individuals and legal entities protecting the rights of consumers, fighting against the unfair competitions and monopoly practices.

Regulation of means of payment in the Civil Code

he means of payments are regulated at least by several acts, namely Consumer Protection Act, Financial Services at Distance Act, Electronic Trade Act, and Money Transfer, Electronic Means of Payment Act.

2. Applicable law – particularities

Credit cards

Laws on credits cards:

• Art. 60. of the Consumer Protection Act, illegal use of a bank card in contracts at distance.

• Articles 27-40a of the Money Transfers, Electronic Means of Payment Act treat rights and obligations of the issuers and holders of the electronic means of payment.

• Art. 249 of the Penalty Code should be revised. It states that means of payment frauds, which cause considerable material damages, are sentenced to imprisonment of 2 to 8 years and imposed with a fine up to the doubled amount of the fraud. "Considerable material damages" mean the minimal monthly wage in Bulgaria multiplied by 14, which is 3080 leva (1540 euro). Hence, the frauds for less than 3080 leva are not covered by art.249. So, the "considerable material damages" should be excluded from the act.

Transfers, Cheques and Payments on line

Articles 27-40a of the Money Transfers, Electronic Means of Payment Act treat rights and obligations of the issuers and holders of the electronic means of payment.

Country	Civil Legislation on Fraud
Czech Republic	Civil Code no. 40/1964, Trade Code no. 13/1991, etc.
Italy	Law 197/1991, section 12 (Undue use of credit cards), Law for the Protection of Data, section 34 (2003), Law of the Cheque, Law for the Computer Fraud (547/2003), Decree n. 112 (30 April 2007): Creation of a Prevention System for the Credit Cards Fraud
Lithuania	Banking Law (2004): Art 56; Transferences Law (1999) Electronic Means of Payment, Cheque Law (1999) and Article 1104 of teh Civil Code (Regulation for the mechanism of the cheque), Law for the distance contracting (2001): Art. 7, 11, 12, 14, 16 y 23; Civil Code (Art. 6366, 6367);
Romanía	Electronic Commerce (365/2002), Protection of personal data (677/2001), Electronic Signature (455/2001), Distance Means of Payment (Regulation 4/2000 of the National Bank of Romania)
Slovenia	Means of Payment Law (Art. 9, 13, 24) ; Banking Law (Art. 230), Chque Law
Slovak Republic	Undue Use of Credit Cards (Law 510/2002, § 25)

ITALY

1. General legislative framework

Consumers' protection in Constitution

Italian Constitution dates back to 1948, a period in which the issue of consumer protection was practically unknown in Europe. Due to contingent political reasons, Italian Constitution is focused on labour and worker protection, rather than on enhancing consumer welfare. A little clue for consumer protection may be found in section 47, insofar as it is stated that "The Republic encourage and protect savings in every form".

Regulation of means of payment in the Civil Code

Italian Civil Code dates back to 1942, a period in which the issue of consumer protection was practically unknown in Europe. Therefore, within the Civil Code, the means of payment are regulated regardless of the subjective quality of consumer or professional. The obligation to pay a sum of money has objective character and one cannot disclaim its liability to pay, unless he gives evidence that the breach of his obligation to pay is due to a material and general impossibility to fulfil the obligation which is not due to himself (Trimarchi P., Istituzioni di diritto privato, XVI ed., Milan, 2005, 300). According to section 1277 of the Civil Code, "Pecuniary dues are paid by cash having legal course in the State at the time of payment and for their nominal value". However, this general principle must be coordinated with anti-money laundering laws, which forbid payment by cash above certain thresholds. In general terms, and further to several amendments (last one has been introduced by section 1, paragraph 1, of Law 6 August 2008, No. 133) it is forbidden in Italy to use cash for payments above Euro 12.500,00 even though lower limits exists for certain specific payments (i.e. payments by cash to lawyers, doctors, etc. are allowed up to the limit of Euro 500,00 until 30 June 2009 and up to Euro 100,00 onwards).

2. Applicable law – particularities

Credit cards

Misuse of credit card is regulated in Italy, since 1991: section 12 of Law No. 197 of 5 July 1991 states that: "Anyone who, in view of getting a benefit for himself or for a third party, illegally use, without being the legitimate holder, credit or payment cards, or any other similar document enabling him to get cash or to purchase goods or services, is punished with imprisonment from one to five years and with a fine from 600 thousand Lira to three million Lira. It shall be equally punished anyone who, in view of getting a benefit for himself or for a third party, counterfeit or modify credit or payment cards, or any other similar document enabling him to get cash or to purchase goods or services or hold, transfers or acquires such cards or documents of illegal origin or any way counterfeit or modified, or payment orders deriving thereto"

This provision is now contained, exactly in the same terms as before, in section 55, paragraph 9 of Law (D.Lgs.) 21 November 2007 No. 231 (who has repealed section 12 of Law No. 197 above), safe for the fact that the amount of the fine is now expressed in Euro currency and ranges between 310,00 and 1.550,00.

The criminal implications of fraud by misuse of credit card seem to be sufficiently covered by this figure of crime, however, in practice, serious problems may arise due to the fact that the author of the frauds may remain unknown, or may reside in remote jurisdiction or, even if Italian national, may be incapable of compensating the victim.

Normal praxis of the card issuer is that of reimbursing the victim of misuse (use of stolen credit card with counterfeited signature or use of stolen data of credit cards and use over the internet without the subscription of the card holder).

Probably this is the reason why the research of the case law does not show any significant civil litigation on the subject, namely the one of victims claiming compensation from card-issuer instead from the author of the crime.

Case law rather focuses on the relationships between the card issuer and shop keepers, drawing a list of obligations for each of them and putting the risk of misuse to one or the other according to various circumstances (e.g. Cassazione civile, sez. III, 14 July 2006, No. 16102, Soc. Trattoria Quattro Venti vs. Servizi Interbancari).

However, a study of the relationships between the card issuer and shop keepers lies outside of the scope of this questionnaire and the conference to be held in Italy shall rather focus on investigating the possible damages for card holders. Indeed, due to the increasing use of the internet, it might well be that card issuers are going to change the above mentioned praxis, by imposing on the victims of the misuse more and more burdens. As far as this kind of problem, please make reference below, to the section on "Payments on line"

Transfers

No peculiar statutes or case law on transfers has been identified.

Cheques

Laws on cheques dates back to 1931 (namely, with Royal Decree 21 December 1933, No.1736) as an implementing device of the Geneva International Convention of 19 March 1931. Therefore, most part of this area relates to uniform law, applicable to all ratifying Member States. No peculiar statutes or case law on cheques, with reference to consumers, has been identified.

Payments on line

This mean of payment, which is strictly connected to information technology, might give origin to so called "computer crimes". For figures and statistics, please make reference to section D) below. How do the Italian legal system cope with this sort of cyber crime? Misuse of credit card is regulated in Italy, since 1991, as explained above in the respective section. Following EC legislation, since 1993, by law 547/93, Italy has introduced a number of provisions of criminal law aiming to punish computer crimes.

Namely, the newly instituted crimes are the following:

• Informatics fraud: similar to the traditional crime of fraud, with the difference that it is committed through an informatics means. Therefore Law 547 of 1993 adds in the Criminal Code, section 640-ter to punish anyone who is seeking to make a profit illegally, through the interference in electronic data processing;

• Counterfeit of informatics documents: to this purpose, informatics documents are considered as traditional ones and section 491-bis of the Criminal Code extends to them the punishments provided for public and private documents.

• Attack to data integrity: the newly introduced section 635-bis of the Criminal Code punished the damaging of computer and telecommunication networks; section 615-quinquies the spreading of virus and malware; section 392 on damages to property now punishes also the damaging of so-called informatics goods

• Attack to the privacy of data and informatics communications: newly introduced figures are the abusive access to an informatics or telecommunication network (section 615-ter of the Criminal Code); illegally possessing and spreading of access codes (section 615-quater of the Criminal Code); disclosure of the contents of confidential documents (section 621 of the Criminal Code) including informatics documents. Also intercepting and disrupting informatics and telecommunication correspondence is now punished by section 617-quater of the Criminal Code, as well as installing of devices aiming to intercept or hinder such correspondence (section 617-quinquies of the Criminal Code).

Finally, it must not be forgotten that there were already old figures of crime, like the one provided for under section 494 of the Criminal Code (substitution of person) which, without any amendment, could perfectly fit to the new cyber crimes, such as the identity theft.

Therefore, the criminal implications of fraud in the on-line payments seem to be sufficiently covered by the various – either old or newly instituted – figures of crime, listed into the Italian Criminal Code.

However, in practice, serious problems may arise due to the fact that the author of the frauds may remain unknown, or may reside in remote jurisdiction or, even if Italian national, may be incapable of compensating the victim.

A first research does not show any significant civil litigation on the subject, namely the one of victims claiming compensation from card-issuers, e-bankers, etc., instead from the author of the crime.

The conference to be held in Italy shall have the purpose to seek to investigate this core aspect and to provide possible guidance for decision of future cases.

Laws on data protection (in Italy, the most recent version of data protection code dates back to 2003) seem to be of no or little effect from a consumer protection perspective, while increasing the bureaucratic burden for the business activity.

In other words, sections 34 of the data protection code 2003 provides for specific requirements in case of electronic data processing, but it does not cover the case in which the e-banker or the card issuer alleges that the breach of data protection is due to the consumer not accurately keeping for himself the relevant data and secret codes.

How can a consumer prove that secret codes were disclosed by the e-banker, rather than by himself?

Some academics is suggesting to extend the principle of product liability, as provided for under EC Directive 85/374 (whereby producers and vendors are considered to be usually liable for damages caused by the products they have produced/sold, unless they prove that damages are due to unforeseeable circumstances), also to the services, like credit cards or e-banking.

This could also respond to economic analysis of the law criteria, according to which damages must lie, in full or in part, with the economic actor who take the largest share of profits in that respective activity (i.e. the card issuer or the e-banker).

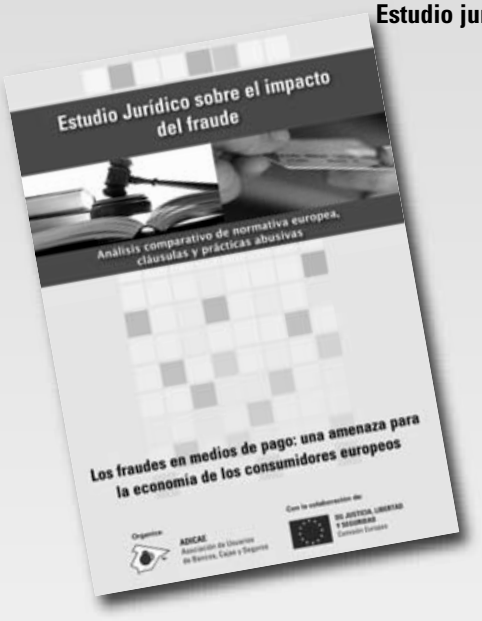
In this way, liability would shift, in full or in part, from the victim of the cyber crime to the companies operating in the sector.

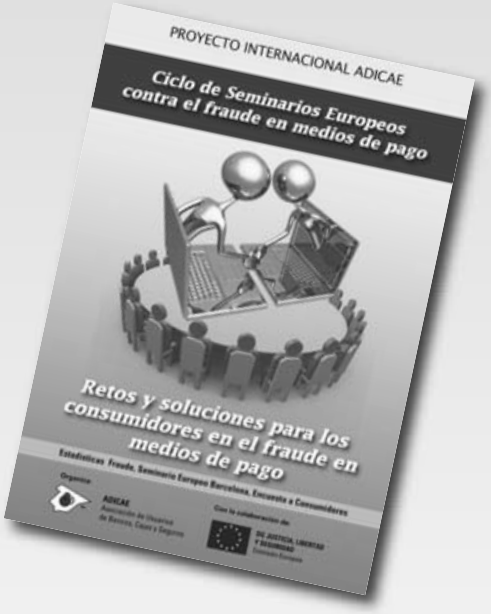
Although we could appreciate and agree upon this suggestion, existing applicable civil law offers very few hints for reaching this envisaged solution.

PUBLICACIONES PROYECTO "CICLO DE SEMINARIOS EUROPEOS"

Si quiere conocer más solicite las publicaciones del otro Proyecto europeo sobre el fraude en medios de pago de ADICAE

Estudio jurídico sobre el fraude

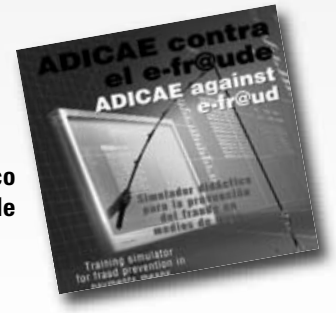




Libro seminario internacional del proyecto

Página web del proyecto

Simulador informático contra el fraude



PART 3

Economic crisis and fraud in means of payment in spain and the european union

Round table about the problems and its solutions

SYMPOSIUM INAUGURATION

■ **D. Manuel Pardos**
Chairman of ADICAE

This symposium represents the final event of a European project that ADICAE has led in conjunction with the organisations, SCS (Czech Republic), FEDERCONSUMATORI (Italy), LNCF (Lithuania), ANPCPPS (Romania), ASC (Slovakia), and MIPOR (Slovenia) for a year and a half, with the support of the European Commission (DG Justice, Freedom and Security).

The use of electronic payment methods is no longer a novelty. For many years, the use of cards in most European countries has been widespread and the number of transactions and the amount of money moved in non-cash payment methods has increased year by year. Spain, as will be shown throughout the various lectures, is a clear example of this increase. "Plastic money" is a payment method that has become widespread for most citizens, especially young people and even children (subject to limitations and control by their parents), who have started to use these payment methods with considerable familiarity. Moreover, the Internet has provided more opportunities for the increased use of payment methods to make purchases, payments and transactions.

Another phenomenon to be included is the mobile phone, which cannot be disregarded. In addition to its various applications and utilities, another function has been developed: its use as a method of payment. Although not currently widespread, it is expected that it will become a popular payment method in the future.

Another factor to be considered is the economic crisis, which is increasing electronic commerce volume and the number of Internet transactions due to lower costs and services made available by advances in new technology.

This makes it possible to develop in new ways, but the downside is that fraud also grows rapidly. As a result, European and national governments have demonstrated their concern about the growing problem of electronic payment fraud and their aim is to reduce the peripheral and non-essential aspects of fraud in these payment methods.

Consumer confidence in payment methods should be taken fully into account, especially in relation to payment fraud and how it adversely affects them. As a result, consumer associations encourage confidence through consumer protection, not only when informing consumers on how to protect themselves from the effects and consequences of fraud, but also to advocate that this change of trend from the use of cash to “plastic money” is much cheaper. It is necessary to reduce costs and commissions in the most popular payment methods, which should be easily accessible in their use and logically more secure. Trust will be reinforced by strengthening the above pillars. In short, before consumer trust can be achieved, protection of their rights and secure use must be guaranteed.

To strengthen the confidence of users, it is necessary for banks to guarantee security and accept that the burden of

proof in cases of fraud corresponds to them. The consumer should only be held liable in cases where it is clear that negligence has occurred. It is necessary for banks to comply with the European Commission's Recommendation of 1988, to which European Associations of Banks and Savings Banks agreed in 1990, through which the cardholder's liability for fraudulent use after theft was set at €150, which is the maximum liability until notification of the loss or theft of the card is made by the consumer.

In this regard, greater concern by banks is vital and greater interest in the opinion of users. I mention this because in spite of numerous efforts made by ADICAE to invite banks to participate actively in the various events, only one of them accepted.

In conclusion, cooperation is necessary between all protagonists in the world of electronic payment methods. It is essential that collective interests have priority, including the users, and that mere economic and competitive interests between companies are sidelined.

■ Dña. Francisca Sauquillo

Chairperson of the Consumers and Users Council of Spain

I believe that this seminar is timely and interesting for its timing, the attendees (representatives from six different EU countries), the topics under discussion and the authority of those making presentations.

The issue of fraud is of great concern. It has always existed, but currently it is developing to an extent that requires all of us to work to curb its progress, hence the importance of a high profile cross-border project to bring together and assess the work completed and the work still to be undertaken. It is necessary to inform, train (through events such as this seminar) and learn from the experiences of different countries to then be able to assess the various solutions and alternatives that can be considered to address electronic payment fraud.

EThrough new technology, this problem has become widespread and global, requiring global solutions. It is not just a problem for a few, but for everyone. We must avoid the individualism that has been produced regarding consumption. It is therefore necessary to circulate information on fraud, just as easily as fraud itself spreads. The more information one has regarding new types of fraud, the better the knowledge and tools to prevent it, hence the need for effective early warning systems so that consumers and users know how to detect fraud.

This seminar is very timely in the new Europe with a new power to legislate, with the accession of new countries with similar general problems but also specific problems. The work of legislators and the different commissions that draft legislation is therefore important as they must remain attentive to the development of fraud in order to propose legislation that is increasingly harmonised and general to deal with a general problem that all European consumers experience as those who commit fraud are well advanced and, in this race, we must try to win, to anticipate the future so that criminals do not achieve their aims.

CHALLENGES AND DIFICIENCIES IN THE LAW REGARDING CONSUMER PROTECTION IN THE FACE OF PAYMENT METHOD FRAUD

■ **Dña. Delia Vaquerizo**
Products and Services Manager at Sistema 4B

In today's society, within the context of the European Union, electronic payment methods have become an indispensable tool for the vast majority of bank customers, for payment in shops, as well as the provision of cash in shops. It is difficult to imagine a world without bankcards. In this environment, it is essential to ensure the stability of the system. Control of payment fraud is one of the factors that must be taken into account in terms of its impact on user confidence. Globalisation, mobility of users and the potential vulnerability of personal data on the Internet and other channels have facilitated the emergence of worldwide organised crime engaged in counterfeiting and the fraudulent use of bankcards.

New methods to combat fraud

Spanish banks are aware of this situation and go to great lengths to provide resources to prevent and deter fraud. As a result of this effort, three Spanish card networks: Servired, Euro6000 and Sistema 4B have experienced much lower fraud levels than the European average, below 0.04% of total sales.

However, in the fight against fraud, all participants must be involved in a coordinated manner, focusing their efforts on four basic concepts:

- Prevention
- Detection
- Detention
- Analysis and monitoring

Payment schemes and banks are actively working with the government in defining standards of security and monitoring requirements that optimise payment method use. Accordingly, to minimise the risk of the physical counterfeiting of plastic, the EMV card has been established as the European standard. The card contains a sophisticated chip with high security levels to verify the cardholder. In Spain, the migration process has already begun.

In European countries where EMV migration is well advanced, its effectiveness has been demonstrated with a reduction in fraud when the card is physically present, although the movement of criminals to areas of the world where the EMV standard has not been recognised has been identified (mainly Asia and America).

Moreover, the new standard does not protect against fraud in electronic commerce and distance selling, which is experiencing growth in line with increased activity in this area.

To protect the cardholder who purchases online, there is a security standard (3D Secure) that certifies the user before his bank for payment through the Internet. Businesses that are classified as "secure", require the cardholder to use the certificate to verify his identity before authorising the transaction. To obtain this certificate, the user must contact the card-issuing bank, usually through its website. It should be a voluntary initiative by the user. Banks can carry out promotional or informative campaigns, but the issuing of the certificate must always be initiated by the cardholder. Businesses that do not apply for this certificate are classified as "insecure" and must accept a delay in the transaction if it is reported as false by the cardholder.

With respect to distance selling, the user must give the three-digit code that appears on the right side of the signature panel to confirm that he is in possession of the card. This number should not be given in writing or by telephone for any other purpose than for a purchase transaction.

How to prevent a crime being committed?: prevention measures

Another major concern of banks is where and how cards are copied. In many cases, the copy is made at an ATM in which a device for copying cards has been installed. European banks have recently published a set of recommendations for banks with ATMs, designed to increase security and reduce the risk of such attacks. In the case of Sistema 4B, these practices are applied as standard to enhance TELEBANCO 4B's network security. Nevertheless, if the user identifies any foreign element in the ATM, he must inform the bank or Sistema 4B directly as soon as possible.

Despite these preventative controls, Sistema 4B and other national payment schemes monitor the activity of the cards through intelligent systems to identify suspicious behaviour indicative of fraud. If there is suspicion of fraud, the cardholder is contacted to establish if a risk exists. If it is not possible to contact the owner but the risk of fraud is very high, the card may be temporarily blocked in order to prevent a financial loss. While sometimes this may cause inconvenience for the cardholder, it is considered as a lesser evil to protect the customer's interests.

Many banks offer customers a complementary information service by SMS, which is highly useful in reducing fraud. The experience of the Sistema 4B banks that have used this service for their customers is very positive, with reductions of up to 40% in defrauded amounts.

Despite all the measures described above, fraud can still occur. The immediate reporting of the fraud by the victim to the Police and bank is essential to enable the identification of the criminals, their location and their patterns of behaviour, information that is transferred by the banks to their intelligent prevention systems. Users should regularly monitor their account statements to identify fraudulent card activity as soon as possible. From the moment that notification is made to the bank regarding fraud or theft, the bank becomes liable for all financial losses. Furthermore, the new European directive regarding payment methods, which enhances cardholder protection, sets a €150 liability limit for cardholders, over which the bank is liable for the financial cost of the fraud.

Actions and measures for prevention, detection and information analysis:

- Secure procedures for issuing and distributing cards and PINs.
- Issuing and distributing deactivated cards prior to activation by the cardholder through authentication procedures.
- Monitoring of internal and random marks that are updated during each transaction, which help to identify quickly if a card has been falsified.
- Monitoring and continuous updating of blacklists of cards that have been blocked because of theft, loss or forgery so that they cannot be used again.
- Monitoring of transactions almost in real time against intelligent fraud patterns that warn against changes in the behaviour of the card, thus detecting any anomalies before notifying the customer.
- Notification (optional) via SMS for the cardholder to check transactions.
- Continuous analysis of fraud cases of all member banks to identify common fraud patterns to train monitoring and warning systems.
- Historical analysis of card activity to identify copy points. Procedures for preventative action against potential counterfeit cards. This is a preventative measure.
- Certification and activation of implementation policies for secure terminals, i.e. ATMs and points of sale so that they cannot be manipulated to copy cards (skimming).
- Compliance with all PCI (Payment Card Industry) standards for the protection and confidentiality of processed data.

Conclusions and proposals for preventing fraud

In short, in recent years, the fight against payment fraud has become a priority for banks, regulators and payment processors, who are aware of how fraud causes mistrust in the use of cards. All of those involved in the system are essential for the control of fraud and the protection of users and the system:

■ The users, following good practice and recommendations regarding the safe use of bankcards.

■ Businesses, respecting the established operational system, requesting cardholder authentication and immediately reporting any suspicious behaviour.

■ Payment schemes, banks and payment processors, as well as regulatory bodies, defining and updating the fraud protection policies, monitoring the implementation of established security standards, sharing information on fraud and actively participating in the definition of new standards and protection mechanisms. Accordingly, Sistema 4B strengthens the exchange of information concerning fraud and shares advances in this field, both nationally and internationally by participating in institutions dedicated to combating fraud.

■ The Police, supported by information provided by the schemes and banks and cooperating with other national and foreign security forces.

■ The prosecution authorities, demanding the highest rigour in resolving cases.

ayment methods are and must continue to be a secure service for bank customers as a means of accessing money. Customers should be aware that they are protected against fraud because risk is minimised with preventative measures and liability is limited in the event of fraud.

■ **Dña. Daniela Bulcu**
Chief Prosecutor of the Romanian Ministry of Justice

The emergence of the first computers over 50 years ago started a real revolution for society. The first major consequence of improved technology was the transition from industrial society to information society. Humanity has experienced great change in this time. As a continuously improving technological tool, the computer has become a normal part of our lives, and is present in all aspects of economic, social and cultural life.

Technological development and wide scale use of computer systems has advantages but also risks. The dependence of companies, governments and individual users on computer systems makes them more vulnerable to the impact of crime. Computers have also become an attraction for those who wish to gain undeserved benefits. Thus, the first computers were used to commit small crimes, and later to commit new forms of crime that were more advanced and specific to computers.

Cybercrime: a current phenomenon

Computer crime is a phenomenon of our times that is becoming increasingly well known as a result of its rapid spread and also in terms of its economic and social consequences. One study has shown that people's fear of computer attacks is higher than any other type of fraud or petty theft. The pursuit of computer crime is still in the process of improvement as only a small number of crimes involving computer systems are recognised by the prosecution authorities.

While it is possible to describe the type of crimes committed in the IT field, it is still considerably difficult to count the losses caused by these crimes, as well as the exact number of crimes committed.

In 2003, the Romanian Police investigated some 200 computer crimes, 50% of which related to fraudulent electronic auctions, 30% fraudulent online orders, 10% unauthorised access to computer systems and 10% child pornography.

Romania's accession to the EU: consequences of anti-fraud regulation

Based on the premise that computer crime can cause many problems in modern society, Romania has applied to its legal system legislation on computer crime, which corresponds to international conventions and standards. Therefore, in order to transpose the obligations assumed as a member country into national law, Romania ratified, with Law 64/2004, the Convention relating to computer crime adopted by the Council of Europe in Budapest in 2001. Romania also agrees with Recommendation R/95/13 of the Committee of Ministers, which took place on 11 September 1995, regarding criminal procedure problems related to information technology.

Accordingly, to comply with the European Union, Romania has adopted new laws such as Law 365/2002 concerning electronic commerce. Article 2 of the law defines its purpose and scope. Through the provisions of Articles 24-28, the following actions are punishable: the falsification of electronic methods of payment, the possession of equipment with intent to falsify such instruments, the making of false statements in the issuing and use of electronic methods of payment, the making of fraudulent financial transactions, the acceptance of fraudulent financial transactions. These offenses are punishable by imprisonment of 1 to 12 years. These two regulations complement the provisions of Law 39/2003 concerning the prevention of and fight against organised crime and Law 21/1999 regarding the prevention of and fight against money laundering. In 2003, Law 16 concerning the prevention of and the fight against computer crime was adopted. Computer crime is defined by Article 49 of this law as the act of causing harm to a person by entering, changing or deleting computer data, by restricting access to such data or by impeding the operation of a computer system for the purpose of obtaining a material benefit. The crime is punishable by imprisonment of 3 to 12 years. The victim can be an individual or a company whose computer system has been affected. It should also be noted that mere intention is also punishable under this legislation.

Future trends in computer crime: the Romanian Ministry of Justice's solutions

Data analysis of computer crime shows the future trends of these crimes, trends that represent new boundaries for those who organise activities to protect the consumer (such as authorities, companies, analysts, consumer associations).

Computer crime directly affects society, which is increasingly dependent on computers. The important aspects of our social life are coordinated by networks and computer systems. As a result, attacks through and aimed at computers will multiply in the future and computer crime will be able to be committed by virtually anyone as computer systems become accessible to most people as prices fall, thus affecting thousands of people anywhere in the world (globalisation of fraud).

In order to address the problem of cybercrime, the institution I represent, the PROSECUTOR'S OFFICE of the SUPREME COURT OF CASSATION AND JUSTICE, the specialised Department of the Ministry of Communications and Information Technology and the Department for Combating Computer Crime within the Ministry of Defence, has created an “eFraud" website that enables anyone to report a possible fraud or other illegal activity to the authorities.

International cooperation

Due to the anonymity offered in sending encrypted messages and its transnational nature, information cannot be controlled, and for this reason, fraudsters prefer to commit computer crime. As a result, Romania is highly active in the field of international cooperation to deal with this issue. Chapter 5 of Law 16/2003 concerning international cooperation stipulates that the Romanian judicial authorities must cooperate, in accordance with the provisions of the law and international legal instruments to which Romania is also party, with similar institutions in other countries and with international organisations in the field.

To ensure that international cooperation is immediate and permanent in combating computer crime, there is a permanent point of contact, the Computer Crime Service within the Directorate for the Investigation of Organised Crime and Terrorism (DIICOT). DIICOT was established by Law 508/2005 and is the only department within the Public Ministry that specialises in investigating and combating terrorist and organised crime offenses. It was created to disrupt and eliminate the cross-border activities of national organised crime groups, which commit serious crimes. As part of the international cooperation, foreign authorities may request this Service to immediately preserve computer data or computer traffic data relating to an existing computer system within Romania. To do this, the foreign authority has to make a request for international judicial assistance in criminal law. In turn, the Romanian authorities can send the competent foreign authorities information and data in their possession that could be necessary to uncover crimes committed through computer systems or that are needed to solve cases related to these crimes.

With regard to Law 161/2003 concerning the prevention of computer crime, various articles are included that state that authorities and public institutions have responsibilities in this area, service providers, consumer associations and other representatives of civil society that develop prevention activities and programmes to combat computer crime. All of these bodies organise information campaigns on computer crime and the associated risks for computer system users

In Romania, the Ministry of Justice, in cooperation with the Ministry of Administration and Interior and the Ministry of Communications and Information Technology develops and continuously updates a database on cybercrime. At the same time, it regularly directs surveys to identify the causes and conditions that favour fraud and cybercrime.

Conclusions and proposals

believe that there should be a balance between law and social reality in this area, because at the moment they do not correspond to one another, hence, for legislation to be effective in protecting citizens, its adaptation to reality should be as fast as possible. It is necessary for the procedures of drafting and passing regulations to be much more dynamic and rapid in order to reflect reality as much as possible and to regulate it effectively.

Moreover, the representatives of civil society and consumer associations have an important role in educating the public about the risks to which they are exposed. Consumer associations should encourage victims of crime to inform the authorities about these crimes. As mentioned earlier, many of these crimes remain unreported to the competent authorities, which means that they are not investigated and therefore remain unpunished.

COMBATING THE NEW TYPES OF ECONOMIC AND FINANCIAL FRAUD

■ **Dña. Nieves Gamoneda**

Inspector of the Economic and Fiscal Crime Central Unit – LAW ENFORCEMENT BODY (NATIONAL POLICE)

B.I.T.: Specialised unit. Functions.

Public safety is a necessity that must be guaranteed in any social environment, including the internet. Consequently, the Technological Investigation Brigade (BIT) is born, which is the police unit in charge of responding to the challenges of new crime forms, such as child pornography, criminal actions and internet fraud, fraud in communications, cyberspace attacks, piracy… Its mission involves obtaining proof, prosecuting criminals and taking them to court.

The basic functions of BIT are direct complex investigations, coordination of operations involving different Police Headquarters, the training of national police officers and other members of foreign police forces as well as international representation, execution and coordination of the investigations carried out in other countries.

Section specialization and division

The B.I.T. is divided into 2 operative sections and 1 technical section. On the one hand, one of the operative sections is in charge of investigations in three sectors, which are the following:

■ MINOR PROTECTION, related to crimes against minors, child pornography and, more specifically, production of child pornography.

■ RAUD IN TELECOMMUNICATIONS, fraud in landline telephony, mobile telephony, injuries and calumnies that are normally carried out.

■ OPEN NETS, investigation of new in criminal activities, issue of illicit activity reports such as websites that encourage anorexia.

The OPERATIVE SECTION is focused on three activities:

• Internet fraud such as computer irregularities and general computing; the "mixed group" focuses on the investigation of computer crimes and even on identity theft.

• Logical security, security on the web, on general computing.

• Intellectual property focused on piracy investigation.

Finally, the TECHNICAL SECTION carrying out training and research tasks:

■ TECHNICAL SUPPORT REPORTS

■ I + D TRAINING AND RESEARCH

Crime investigation regarding drugs sale which cause serious health injuries.

Fraud by means of new technologies

If we ask ourselves this question: Fraud on the internet? The answer would be that fraud can be carried out by any means facilitating network: WEB sites, Electronic mail, Sales/Auctions portals, Instant message services, Messaging to mobile phones and others: IRC, ICQ, Forums…

The modalities investigated by the BIT are:

• Purchase of products and services by means of valid card numbers (CARDING) where, in order to

commit fraud, the physical card is not necessary, just numerical data is required on the internet to carry out fraudulent acts.

- Fictitious auctions and sales carried out from telephone booths, for instance.
- Fraudulent Electronic Transfers (TEF).
- Phishing.
- Pharming.
- Malicious programmes

Examples of fraud modalities detected by the BIT:

Auctions:

By means of a telephone booth, from Spain, false auctions websites were created and the money would travel to Italy and Romania through a mobile phone. Research about the globalization of this phenomenon is that despite being a crime committed in the Spanish territory there were no Spanish users affected.

Phishing

Users were sent an email replacing the Adicae identity (Banks and insurance consumers' association of Spain) to confirm their bank passwords.

Fictitious commerce, where any type of product is sold. An example of this is the “Operación cargado” (“Topped up Operation”), where it was detected that products were bought through the creation of mobile phone top-up fictitious websites; these websites would appear first positions in search engines and as soon as users provided their card details these were used fraudulently. All these webs were created by minors and they kept in contact by means of IRC private networks

Fraudulent electronic transfers by means of the well-known type of fraud “Nigerian letters”. Countless e-mails which used the so-called old “timo de la estampita” (fraudulent act). Bulk emailing is sent asking for a payment request related to a prize where the authors are African, from where its name is adopted.

Conclusions

■ These types of fraud are executed by highly structured organizations, which are authentic crime multinationals.

■ They use intermediaries for distribution and also carry out fast money transfer operations through poor control circuits.

■ These organizations use servers that are located in third countries, most of them without any type of control and legislation making reference to new technologies, to the information Society and even less to fraud in payment methods on the internet.

■ There are territorial and jurisdictional limitations that obstruct investigations being carried out. However, international collaboration is often used to perform investigations. For this reason, global collaboration is necessary to battle fraud.

■ Identity theft is essential in the economic crime, although this hasn´t grown much yet according to data provided by the BIT.

■ **D. Peter Gouwy**
Intelligence analyst (Europol).

What is Europol? Functions and history.

Europol is the security body of the European Union where 27 EU member States are involved as well as 14 others that are not EU member States and 10 international organizations; Europol is in charge of managing confidential information in the crime scope. Europol´s objective is to significantly contribute to cooperation among competent authorities of the member States that are responsible for the prevention and fight against organised crime and international terrorism.

Europol was established under the European Union Treaty on 7th February 1992, headquartered in The Hague, The Netherlands, Europol initiated its operations on 3rd January 1994 under the name 'Europol Drugs Unit (EDU)' and limited to drug crime.

The Europol Agreement was ratified by all the EU member States and came into effect on 1st October 1998. In response to different legal acts related to the Agreement, Europol became a fully operative body on 1st July 1999.

Progressively other crime scopes were added to its competences. On 1st January 2002 the Europol's mandate was extended to cover all the serious international crime as it is detailed in the annexe to the Europol Agreement. From 2007, other money laundering crimes are also covered.

Europol supports police activities developed in the different member States, mainly focusing on combating:

- Illegal drug traffic.
- Clandestine immigartion networks
- Terrorism
- Currency falsification (Euro) and other payment methods.
- Human trade (including child pornography)
- Illegal vehicle traffic
- Money laundering..

Other primary scopes of Europol's activity are crimes related to violence against other people, financial crimes and cybercrime.

Europol takes action where there is implication of an organized criminal structure and two or more member States are affected.

Europol supports member States by:

■ Facilitating information exchange according to the national legislation amongst the Europol liaison officers (FEE). The FEE are distinguished Europol officer by member States as representatives of their security bodies and forces;

■ Carrying out operative analysis supporting operations;

■ Elaborating strategic reports (e.g. threat evaluations) and analysis of criminal activities, taking into account information and other data provided by the member States and by third parties;

■ Offering specialised knowledge and technical support in the investigations and operations carried out in the EU, under the supervision and legal responsibility of the corresponding member States.

Besides, Europol actively encourages the analysis of criminal activities and the harmonization of investigation techniques in the member States. Europol has direct international collaboration. The Europol network supports 27 member States, 14 non member States; the European Unit collaborates with 10 international organizations. Concerning this collaboration, there are two types of Agreements: An operative agreement, where personal data are exchanged and a strategic agreement where personal data are not exchanged.

There are operative agreements with Norway, Switzerland, Island, Croatia, Austria Canada and USA. Currently, an operative agreement with Croatia is trying to be formalised. Strategic agreement with Albania, Bosnia Herzegovina, Colombia, Macedonia, Moldavia, Russia and Turkey.

Information exchange.

Europol has, in all countries, a liaison officer and a National Unit. There are some analytic work files. The information is received, analysed and sent to Europol National Unit. No information is exchanged with private companies and as for Banks, Visa, MasterCard, the personal data are not received as these belong to the member State. If the information is sent to Europol, it is supervised by the State.

Fraud in payment cards (skimming).

On a strategic level, Europol has elaborated a report on the global problem on the internet, on how pharming or phishing work. The member countries were informed about how to act in cases of Carding.

On an operative level, Europol dealt with the type of fraud called “skimming”, which is a copy of the magnetic band in cards (In year 2009, criminals intercepted 250,000 cards which is almost the amount of cards that were issued in Spain). Automatic cashpoints and TPVs can be manipulated by criminals. Also, “hacking” new cards with a chip (EMV system) was detected. A magnetic band card seems to be better as its chip, for instance, is not used in USA and these can be copied, by criminals, for 60 or 80€. Surely, with technological and logistic advances, shortly, these costs will be cheaper. As for Carding, Europol informs and trains police forces of the member states to deal with these cases. Apart from that, meetings with the private sector are held (financial entities and Payment Systems). There is a security team covering almost all European countries. Europol has also had meetings with airline companies as they are continuously affected by fraud in their cards.

Finally, it needs to be mentioned that Europol collaborates with Interpol and they are creating a collaboration website regarding this card fraud issue.

Data and work files collection plan.

What type of people does Europol collect information from?

The data are referred to people considered "suspects", according to each national legislation, for having committed or participated in criminal actions without the need to have been charged with those crimes and it also affects those people who are believed they might commit a crime in the future.

What data does Europol computerize?

Name, surnames, nicknames, birth dates and places, nationalities, sex and “other useful identification characteristics", crimes, actions attributed "or that might be attributed", sentences and suspicion of belonging to a criminal organization as well as any other “complementary information”. Besides, Europol has created the so-called “Work files”, where it stores, modifies and uses data referred to the people previously mentioned, to people who are considered “possible witnesses” in investigations despite the fact that there might not be an open legal cause, people affected or when there are “reasons” to presume they might be affected”, both “intermediaries and companions” as well as people “who could facilitate information” about crimes.

Once all the information is obtained, it is provided to the National Police of the member States and support is offered to be able to come closer to other countries in order to share information as criminals have no frontiers.

■ **D. Alfonso de Miguel**
Civil Guard Captain (Computer Crime Group)

The citizen contacts the Civil Guard: a sensor of fraud's reality.

There are two mail addresses for citizens to communicate with the Civil Guard about types of fraud they have been victims of. These two mail addresses function as two sensors which provide information about the criminal situation in our country.

With the statistics carried out by means of communications sent to these mail addresses we have come to the conclusion that with the passing of time what varies is the modus operandi and that the communication contacts about these types of fraud have dropped.

Statistics analysis.

Analysing the statistics that we have in our power concerning "Criminal acts and Fraud" we can see there is 48% of B2C criminal acts, 5% of C2B criminal acts, 16% of Nigerian lettes,13% of fraud in telecommunications,2% in carding, 12% fictitious surveys and 4% regarding "Other types of fraud" (partners, online games,..).

We can say there is a continuity concerning year 2008 and that the modalities are still the same but executed differently, what we call "flash fraud".

With regards to Phishing, it has been noticed that there has been a fall in 2008 as for the amount of cases and there has been a decrease in communications due to usurpation of banking WebPages. The victim that suffers this type of fraud does not generally report it; therefore communications about usurpation are disappearing.

The improvement of cybercrime with the passing of time is quite relevant although there are no new types of fraud; the modalities are still the same, but with different execution. Now they focus on improvement in the capture of mules with more studied formulas, for instance, by means of an email offering a job position.

As an interesting fact, we can say that 80% of IT systems are affected by viruses and 40% of computers are compromised by Trojans.

China is the biggest money beneficiary from electronic fraud, with identity theft cases. A fraudulent act is performed by the buyer where a man is selling an item and the false buyer asks all possible details about the sale, once those details are collected he uses them to offer the same item in another country. The "couples" type of fraud, where 6-8 messages are sent from Costa Marfil with spectacular girls asking money for their journey.

Therefore, from the analysed statistics we can conclude that phishing communications have fallen but they are still being carried out as the number of phishing hasn't' decreased and there is specialisation by the aggressor with the automation of the threat by means of banking malware and ignorance by the malware threat user.

Police investigation and cooperation. Jurisdiction impediments.

Criminal acts, fraud and phishing are investigated, but sometimes the difficulty to identify some facts with the same suspect arises. Also micro-frauds are investigated by mainly Romanians who would receive assets in their bank accounts. We can say there is police international cooperation when prosecuting these types of fraud; however when it is about prosecuting criminals an order is necessary, which affects the Ministry of Law and Justice and if a judge doesn't have any jurisdictions, the procedure becomes complicated.

Conclusions

In general, the economic crisis has not been noticed, though the "black number" (cases that are not reported and therefore no proof is ever recorded) might have increased and some variation has been noticed in the modus operandi, confirming the use of Trojan malware in cases of phishing.

Amongst the many measures to minimize the fraud effect in payment methods the following are proposed:

■ Web movement confirmation systems (SMS´s or call centre). Thus, every movement in the users´ account is notified to them in real time, therefore users, in case that an operation has not been carried out by them, will be able to act in order to take the necessary measures and avoid greater damage in their accounts (bank account cancelation by means of warning the financial entity as well as a police report).

■ Preventive blocking of accounts. Sometimes, entities are aware of fraudulent activities but the account is not blocked for security reasons as a report is required, however often that report doesn't happen due to fear. There are people against these preventive blocking of accounts due to the fear of not being able to carry out operations, but it is safer to perform preventive blocking rather than regretting having lost all the money in that account.

■ **D. Diego Alejandro**

Group 1, Payment Methods Inspector at the Police Headquarters, Law Enforcement Body of the National Police.

What is a criminal organization?

Criminal organizations are those organizations having, as an objective, some type of crime or those encouraging it as well as those with the purpose to commit or encourage the commission of organized, coordinated and reiterated misdemeanours. The main criteria in these organizations are:

1.- Collaboration of two or more people.
2.- Distribution of specific tasks.
3.- Continuance in time. (6 months)
4.- Mechanisms of control or internal discipline.
5.- Suspicion of serious crime.
6.- International activity.
7.- Use of violence or intimidation.
8.- Use of commercial or economic structures.
9.- Implications in money laundering.
10.- Political influences, means of communication, etc.
11.- Search for benefits or power.

It is also necessary to mention that these organised bands have a hierarchical structure and their function is well delimited and defined. As for the AGENTS relevant in the fraudulent act, we need to mention the Provider, the Forger, the Passer, the Receiver. Also, we have the figure of the Collaborator who covers a "connivent", the "mules", counter vigilance, the person in charge of laundering money, the front man, etc.

CRIMINAL MODALITIES:

■ Stolen/lost cards: "Hot" cards

■ Cards not received by the holder.

■ False credit card requests in order to obtain physical support and a PIN number.

■ Fraudulent use of numerations (CNP)

■ Card falsification

- Electronic falsification
- White "Plastics" are sold on the internet and used to carry out fraud.
- Alteration of personalization
- Entire falsification

Investigation problems

The territory scope of this phenomenon has an international character as bank cards can be of Spanish origin and be used both in Spain and abroad and, on the other hand, the cards can be foreign and be used in Spain.

Another type of data to take into account is that these International networks have great mobility, that there is an increase in Specialization and Organization of Criminal Groups, which change their telephone numbers and, as a Security Measure, there should be a faster judicial reaction.

Another problem is that the installation of devises is carried out during weekends, bank holidays and holidays, and in other occasions the time from cloning to the moment when the fraudulent act is detected is too long. It is clear there is lack of collaboration among establishments when it comes to facilitating recordings and recognition and also lack of collaboration from Financial Entities as the responses are slow and the information is incomplete or even inexistent.

Obstacles for the prosecution of criminals

The lack of preventive measures in some financial entities is clear: absence of security cameras (which can actually record), the recordings are poor quality, lack of periodic checking of cash points and installation of detection technical systems, etc. Concerning fraudulent movements abroad, the National Police faces the inaccuracy of information and the lack of judicial and police collaboration in other counties. To these problems, the use of the internet is added, which means the favouring of anonymity, connection to wireless networks and connections performed in cybercafés or telephone booths.

Crime financing and internationalization.

It is characteristic the fact that behind these crimes are criminal organizations using this defrauded money to finance other types of crime: falsification of documents, number plates, theft and upmarket vehicle sale, drug (distribution and promotion), arms, etc. It is then a rule for these organizations not to only focus on crime in payment methods but on diversifying "their business". Also, the fact that they are international is characteristic both for the composition of their members as well as places for operation and/or to commit different criminal activities.

Conclusions and proposals

The criminal collaboration among the different police forces in the same country is absolutely necessary, as the heterogeneity of criminal acts committed by these groups is a fact. Besides, the collaboration among different police forces from different counties is necessary and Europol and Interpol must coordinate the management of all information facilitated by these police bodies.

However, although this collaboration might be totally effective it would be nothing without the judges' intervention and the justice administration of the countries involved. After carrying out investigation, the collaboration and intervention of judges who have capacity to judge with the normative adapted to the current times is necessary. Many of the cases investigated and detected ended up not being judged or prosecuted by justice due to the fact that these judges are not competent to deal with these acts due to the current regulations.

LIMITING LIABILITY IN CASES OF FRAUD: THE MAJOR OUTSTANDING QUESTION FOR USER CONFIDENCE

■ **D. Alejandro Salcedo**
Coordinator of the Consumer Institute of Castilla La Mancha

The growth of fraud in the Information Society

In a world in which different payment methods are becoming more and more common for any type of purchase, including the most mundane, it is becoming increasingly necessary to guarantee the security of these payment methods. Fraud is a growing threat in our society, in which technology plays an ever greater part, and it is this technology that is directly responsible for an increase in fraud, fraud that is as diverse as it is widespread and based on one of the new pillars of our society: the Internet.

Apart from the dominant characteristics in any type of fraud that consumers are currently facing, there is the added situation of the economic crisis, which drives criminals to take advantage of the precarious situation of some consumers (situations that are common to many) to commit fraud: job offers, gambling, lottery, philanthropy etc.

Existing legislation

Within this context, it is necessary to point out which laws govern these fraudulent activities. The first that I would like to mention is the Recommendation by the European Commission in 1988 to which European Banks and Savings Bank Associations agreed to comply in 1990. This stipulates that the cardholder liability for the use of a stolen card shall be limited to €150: the current limit applicable after the notification of card theft or loss. In the majority of cases of falsification or theft, the incident must be reported within 24, 48 or 72 hours.

The role of government

As is the case with many other participants, government must take an active role in consumer affairs. However, in order to act correctly in the eradication of fraud, several current lines of thinking should be clearly understood:

- The functions of consumer affairs administration are currently limited to hearing and mediation. Added to this is the fact that several different bodies may become involved in a commercial transaction in which payment fraud may be committed and even different areas of competence within a single body, quite apart from the involvement of state law enforcing agencies. This can lead to a conflict of interest between different agencies.

- Government obviously has limited resources. The techniques for committing fraud are far in advance of current government capabilities of combating them. The costs involved in taking preventative action in fraud cases.

–The mechanisms involved in the resolution of consumer cases are insufficient. Moreover, the lack of laws is self-evident as are the difficulties in resolving the situation to the satisfaction of the consumer.

The following must also be taken into consideration: DIRECTIVE 2007/64/EC BY THE EUROPEAN PARLIAMENT dated 13 Nov 2007 on electronic payment methods in the domestic market, modifying Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and replacing Directive 97/5/EC. The objective of this directive is to lay down the necessary legal framework to create an integrated payments marketplace, i.e. to create in Europe a unified payment area through the implementation of SEPA (Single Euro Payments Area,), whose objective is to extend the use of electronic payments in the same way as exists for coin and note payments. Finally, it intends to establish a level of data protection and to define the rights and obligations of the users and payment service providers. The purpose of this law is to be incorporated into the Spanish legal system. The law will become effective on 1st November 2009. This law will consolidate and clarify common banking practices.

Finding the criminals is extremely difficult and the banking institutions do not want to assume the responsibility of doing so.

– Lack of coordination.

– Unrealistic consumer expectations. There is palpable consumer discontent with the current situation in respect to payment fraud.

– Currently, the question of payment fraud is an unresolved issue, despite its obvious magnitude.

Action proposals

Given the current shortcomings in this question, several solutions must be prioritised simultaneously:

Assumption of co responsibility, closing loopholes.

Preventative policies:

- The need to carry out an in-depth study of the situation..
- Programmed monitoring:
  - Network security protocols.
  - Website tracking.
  - Documental analysis
  - Mystery Shopping
  - Electronic security alert network (which must be accompanied by blocking activities)
  - Dissuasive measures (reports; publicity; sanctions ;…).

– Protective policies.

• The establishment of mechanisms for resolution and ad hoc compensation (arbitration; consumer affairs; systems of guarantees ;…).

• Inter and intra-administrative coordination.

• Concerted action.

– Facilitative policies.

•Provision of resources.

• Information and publicity.

• Public awareness campaigns.

• Training courses in the use of networks.

• Financial education programmes.

• Positive discrimination strategies (distinctions, accreditations etc).

• Special attention for at-risk groups (the handicapped, the elderly, immigrants, the poor, the uneducated,…).

■ **D. D.Pablo Mayor**
Lawyer on the ADICAE legal team

An examination of liability and subsequent limitation in cases of fraud pre-supposes:

■ The existence of a situation in which any party in a legal or commercial exchange (we shall concentrate on consumers and users) has incurred losses or damages.

■ The existence of an action directed against the PROPERTY of the consumer [who finds his interests interfered with in some way].

■ The need to buy the interests in question with the aim of determining which operator is responsible, which has been imprudent or has taken part in bad practice.

■ In conclusion it can be seen that the determination of liability in cases of fraud is an eminently logical operation and in the majority of cases, judicial.

From this, two questions can be formulated:

1st.- Who is held liable in a financial fraud situation?

2nd.- Is the consumer always liable?

This is the common perception, it is maybe a slightly PESSIMISTIC view, and far from realistic

A real case history: In ADICAE we have a case of a person who charged several transactions to his card. Upon investigating the origin of the payments, we reached the conclusion that there was postal traffic between the banks that stated the account numbers, which, together with the DNI and an address meant that payments were authorised. Evidently, and without the need for further investigation, it is clear that the bank had acted negligently in permitting other persons to gain knowledge of an account number without taking the barest of precautions.

Everybody knows about the risks involved when DISTANCE SHOPPING (e.g. catalogue shopping) as well as ELECTRONIC - one of the specialities of distance-contracting.

Credit card security is a controversial issue – this is a widely used payment method with evident fraud risk-, particularly with respect to cloning, PIN theft etc. In general, the security system for credit card payments is controversial given that in law, security and economic gain are juxtaposed (greater system security means greater investment and lower profits).

This leads to phenomena such as:

- "Phishing", the acquiring of PINs via false messages (active fraud system)
- "Pharming", alteration of the user's browser bar, which means that when he accesses an on-line bank or shop, he is seeing a false web page (passive fraud system).
- Cloning and duplication of cards which accounts for approximately 10% of credit card fraud
- Card theft (by traditional or the now well-known Lebanese link method
- Acquiring of PINs via e-commerce or on-line banking.
- Others.

It is a system that the banks claim is secure yet we all know it is not one hundred percent secure.

As an example of judicial treatment, Ruling 101/2004 of 23 November in the Provincial Court of the Balearic Islands (Section 1) can be cited. It states: "It can be deduced that there is a victim, the bank, which provided the accused with the T.P.V., (…); and there is a loser, who is not the cardholder, because when he refused the payment and the card supplier turned to the bank who facilitated the Point of Sale terminal, the bank produced the slips signed by the cardholder, when the bank realises that it has been the victim, it cannot logically then present signed slips when there has been no transaction, therefore they must return all monies to the card supplier, bearing the losses that were incurred before the fraud was discovered".

This example serves as a starting point for the attribution of liability: as the system is not 100% secure, it operates on the assumption that the banks must bear

the losses and damages just as they reap the profits (ease of use) from e banking. Although the courts normally follow these criteria, the economic implications obstruct access to justice for the individual, by making any eventual claims against the bank difficult by the simple fact that the individual must bear the legal costs involved by taking the bank to court. (Apart from the outlay, the claimant must invest in order to recover).

ADICAE and other associations, after the necessary out of court processes, apply the principal of "who claims pays": when there is knowledge of a presumed crime it must be reported (in fact, in many cases, fraud goes undetected by virtue of the fact that the quantities involved are so small as to go unreported); on the other hand, the bank often uses this fact to show that the claimant has not tried to find the person responsible, therefore trying to avoid the civil responsibility deriving from the crime.

Bearing the above in mind, the existence of fraud has necessitated the establishment of preventative and reparative safety systems.

■ Preventative these are the protocols that the banks establish to avoid fraud. As an example of fraud prevention in other countries (the UK and France, for example) a payment system using MOBILE TPV UNITS is typically used, where the user enters his PIN at the point of sale or goods delivery, while in Spain the card is still used. This system is ideal to avoid the ever more urgent problem of cloning

■ Reparative, on the other hand, are the methods used by the courts to "compensate" and restore a situation of fraud. This is where the problem of over-legalising arises, as the principal obstacle that the consumer finds (requiring the setting up of out-of-court reparation systems that are quicker and cheaper).

In the order of things, and particularly in the context of e-contracts, card payment for on-line services generates a certain lack of confidence. The fact that the consumer must transmit his PIN over the internet leads to justifiable concerns that the details may be CAPTURED by third parties and used fraudulently.

It would pay to reflect on how often we have seen warnings about working on-line with an insecure connection and how many cases of fraud we know about personally. It is clear that the basic problem in these cases is the fact that neither party are present simultaneously which impedes the identification of the cardholder as well as the service or goods supplier, opening up a vast field of opportunities for those who wish to commit fraud. Add to this is the fact that there is not even a signed receipt by the cardholder and we find ourselves with the simultaneous advantage and drawback of anonymity and the abstraction of safety measures.

It must be pointed out that, in the experience of consumer associations, and in particular ADICAE, we find that **THE BANKS ARE NOT INTERESTED IN A COMPLEX (SAFER) SECURITY SYSTEM WHICH WOULD MAKE IT LESS APPEALING TO CLIENTS**, having already discounted several systems and projects either for reasons of cost (fingerprint or iris recognition) or for being excessively complex.

In the experience of ADICAE, the supplier limits himself to asking the client for the card number and expiry date and possibly the last three digits of the security code that appears on the back of the card for international transactions. However, it is current practice to require the entry via a keyboard of the card number or PIN when making a payment, which guarantees the security of the transaction. Therefore fraud requires previous knowledge of the nineteen digits and expiry date of the card. **PREVIOUS KNOWLEDGE** would not appear to be too difficult, given the expansion of the use of so-called malware designed to obtain user data or a Trojan Horse that will install itself on the computer.

In relation to credit cards, legislation protects cardholders against improper or fraudulent use in on-line transactions and there are now **PENAL SENTENCES** handed down. Regarding criminal legislation, art. 248.2 of the Criminal Code typifies I.T. fraud and considers "guilty of fraud those who, for illicit gain, and through I.T. manipulation or similar, obtain an unauthorised transfer of funds to the detriment of a third party" This obviously includes the duplication of credit cards.

On the Civil statute books, art. 106 of the Condensed Text of the General Law on Consumer Defence regulates card payments should be read in order to understand the protection that the legislator grants to consumers. Upon reading said article, it can be inferred that the cardholder whose PIN has been improperly used by a third party has the right to **CANCEL THE PAYMENT BY THE CREDIT AGENCY**, to take effect no later than 30 days from notification of the cancellation. This possibility grants the consumer the safety of knowing that they will not be held liable while the facts of the case are under investigation. In addition, in accordance with jurisprudence, it is the supplier who bears the burden of proving that the card number used to pay for the services was introduced by the cardholder. In this respect, there is an inversion of the burden of proof to the benefit of the consumer, which represents a vital backup to Internet transactions, which is of prime importance, given the growing popularity of these systems. The issuing bank is only responsible for fraudulent or improper use of

the credit card if this use infringes on the contract signed by the holder, as was mentioned in the opening paragraph. It is evident that negligent behaviour by the cardholder makes him responsible to the supplier and bank for damages incurred (e.g. for having given his PIN to a third party or for failing to inform the bank of loss or theft), and holding him liable, e.g.: *WRITING THE PIN ON THE BACK OF THE CARD.*

In view of the above, it can be concluded that the cancellation of a payment considered fraudulent can be requested and that in the face of such a cancellation by the cardholder it is the service provider who shall bear the cost of the operation, without the holder having to prove whether the card number was introduced by him or fraudulently by a third party. The cardholder is protected if damages have not been incurred.

In other cases and if there have been damages incurred PROTECTION IS AFFORDED ONLY THROUGH THE COURTS. Given that the Client Protection Services of the banks as well as the Complaints Procedure Department of the Bank of Spain and the CNMV never include in their reports references to damages caused to consumers, which are fixed by the courts, with the exception of those case where the banks settle out-of-court to avoid cases.

It has been demonstrated that before the specific nature of many contracts and the clarification of many consumer aspects, technical decisions from the Governing Bodies prevail, making OUT-OF-COURT ASSESSMENT fundamental, particularly in the formulation of complaints to go before the supervisors in order to establish the bases for legal recognition of the responsibility.

With reference, once again, to the security systems, it must be remembered that in transactions, the issuer must give the holder the PIN, which gives greater security when buying on-line. In on-line transactions, the introduction of the PIN (AND NOW THE USE OF A KEY CARD, GIVEN BY SOME BANKS AS A BACKUP SECURITY MEASURE) supposes the identification of the cardholder, necessary for the correct functioning of the system. The bank accepts transactions with the PIN as long as the account holder has the funds and the card is valid. These systems, the PIN and the key card to combat malware represent a way for the banks to avoid responsibility. Although it must be pointed out that greater system security will result in a benefit for the client as well as the bank, which will no longer have to bear costs for lack of proof.

IN THIS CASE, THE PROOF OF NEGLIGENCE IN THE USE OF A PIN OR IMPROPER CUSTODY OF THE CARD CAN EXONERATE THE CREDIT AGENCY. E.g. ***If a card is given to another person.***

In fact this is the reason normally used to justify failing to answer client's requests..

Another case from the Association's archives: that of a father with two children who both have savings accounts in a bank. An unauthorised transfer of the daughter's funds to a third party took place and it proved impossible to have the funds returned to the rightful account. Then the same thing happened with the son's account, but the transfer was stopped. The bank, in order to avoid responsibility, demonstrated that improper use of the father's PIN had occurred. The case had to pass through the Ombudsman, the Bank of Spain, and then to court. A settlement was finally reached on the court steps three and a half years later.

In this case there is the problem of there being no transaction: the bank appeals and that at least three and a half years go by before the money is returned, making the process extremely expensive. This behaviour is within the law yet hardly ethical within the terms of corporate responsibility so fervently lauded by the banks.

Even if the cardholder had acted negligently in giving his PIN to a third party, or failing to notify the issuer of the loss or theft of the card, he could still cancel the transaction, although he would be held liable for any losses or damages arising.

Another case resolved in April 2006 in the Provincial Court of the Balearic Islands was that of a cardholder who demanded the refund of a payment that he did not recognise, that had been made through a card issued by the bank but that the client claimed never to have received. The bank refused saying that the card had been sent, although they had no proof of receipt.

Relating to credit card issuers, Framework Decision JAI/413/2001, dated 28th May, by the EU Commission relating to the fight against fraud and falsification in payments other than cash, defines payment instruments. Viz. Articles 1 and ss. For the definitions.

For a fuller understanding, Consultation 3/2001, dated 10th May, should be studied. This qualifies in legal terms, the use in public call boxes of electronic instruments that mimic prepay cards; Consultation 4/93 that confronts the problem of the legal situation surrounding fraudulent manipulation of day cards on public transport.

Regulations relating to card use in Spain are founded on contractual freedom as laid down in arts. 1091 and 1255 of the Civil Code, as there is no positive legislation on credit cards, not even of an administrative nature.

In the face of this lack of regulation, the main problem arises with card theft, as the agreed conditions

establish the obligation of the cardholder to inform the issuer within a fixed period, by phone or in writing.

IN THE CASE OF FRAUD

The problem that arises is who is responsible for the loss in the case of an invoice bearing a false signature. According to the EC Recommendation dated the 17th November 1988, up to now the limit of responsibility is fixed at 150€ after notification.

This Recommendation, despite not being binding, has been accepted by the majority of banks in Spain. It is therefore normal that a credit card contract contemplates that before said notification the cardholder is responsible for a certain amount, except in the case of fraud or grave misconduct. In any case, after notification, the responsibility rests entirely with the credit institution and **IT MUST FALL WITHIN THE LIMITS ESTABLISHED AS AN ADDITIONAL SECURITY MEASURE.**

One of the problems typically faced is that of the small nature of sums involved, which make them difficult to trace.

CONCLUSIONS

In view of the above, it can concluded that although the on-line banking systems are relatively secure and that the consumer is reasonably protected against fraud and attacks on his bank accounts, there is still a long way to go before there is 100% trust in Internet operations. As a first defence that could be employed to improve and restore clients' rights in those cases in which their legitimate rights have been obstructed, ADICAE and other associations are pushing for the establishment of out-of-court systems for the resolution of these conflicts which would grant freedom of access to a tribunal for all those who require it. The small sums usually involved make it unviable for claimants to pursue a claim through the courts therefore meaning that the majority of these cases remain invisible yet ever more frequent.

In Spain, legislation including art. 106 of the Condensed Text of the General Law for Consumer Defence that regulates card payments, the user defence system united with the principle of the inversion of the burden of proof, added to the fact that the courts are ever more sensitive to Consumers' Rights which is the subject of much jurisprudence is all beginning to regard consumer rights in a reasonably favourable light.

Notwithstanding the above, the role of the Associations including ADICAE (pioneer in financial fraud cases) is becoming more and more necessary. Of particular importance would be consumer education, as a way of avoiding these situations and the formation of collectives as the best form of defence against all these types of fraud that claim hundreds or thousands of victims.

IMPACT OF THE ECONOMIC CRISIS AND FRAUD IN ONLINE PAYMENTS AND ELECTRONIC COMMERCE

■ **Dña. Elena García Díez**

Coordinator of e-Fraud of INTECO (National Communications Technology Institute)

Introduction: Information Society Development

In order to assess the impact of the economic crisis in online fraud and electronic commerce, it is necessary to focus on the evolution and development of the information society. The use of electronic methods of payment registers a clearly rising trend. At the same time, the level of development of electronic commerce and its different methods of payment also rises. The number of Internet users or consumers surfing on the Internet and using it for buying is rising, so there is a bigger diversification of the use and the type of purchases. Apart from the fact that the availability of some services is far away of being considered optimal, it is noticeable the trend to develop services aimed at citizens more than at companies (24 million of Internet users and 7.6 million homes connected in Spain) and the attention paid to the concepts linked to the generation of income.

Day after day, Internet includes a bigger number of work-related, professional, personal and leisure activities of Spanish consumers. 41% of houses in Spain already have an Internet connection. Initially, consumers used the Internet for simple tasks, such as communication among them and research of information. Nevertheless, and despite the fact that this activities register a high level of activity, consumers start doing more complex and transcendental tasks. This way, it is frequent to see how they plan and book trips, look for a job or have access to online education to find it, get any kind of product or do banking operations such as raising a mortgage.

However, we should emphasize the fact that availability or diversification in the Internet does not automatically imply its use. Internet access is a necessary condition, but not necessary enough for the development of Information Society.

Culture of User Security and the use of secure solutions at home

Incidents related to security and trust of the user on the Internet are a critical factor that determines the development of the Information Society in Spain delaying the adoption and extension of the services through the Internet, such as electronic commerce, electronic administration or online banking.

In relation to information security, Internet users apply security measures without active participation (automated); this causes the existence of a deficit in the incorporation of measures that demand bigger pro-activity on the side of the user.

Among these tools, antivirus software is the most generalised one. Some of the most important reasons to avoid the implementation of security measures are those derived from the lack of knowledge or from the feeling that it is not necessary. It is remarkable the fact that a big percentage of users who do not use antivirus software, claim not to use it because it slows the speed of the PC or the Internet surfing.

Concerning the effect of the users incidents, the most common consequences are updating, renewing and installing new projection barriers (10% of the users installed the first antivirus and 20% change it), change of opinion and behaviour concerning security, being more prudent and claiming more implication on the side of public administration. At this point, it is important to know that, due to the essential character Internet has now, incidents barely modify the use of services.

Although almost half of the homes show that they would use more services if they knew how to decrease the risk, the analysis indicates that, in general, incidents related to security do not make users abandon the services or stop using the Internet. But there is a delay effect in the incorporation of Information Society related to the lack of trust on the Internet. This effect has to be found in the “non-users”, that is, those who do not feel protected enough as to join and move freely on the Internet.

This way, common Internet users have embraced online services in their own lifestyle so that it is very difficult for them not to use them. In this context, incidents are interpreted as warnings to increase the protection equipment and/or to be more prudent with their habits, but they are not interpreted as warnings of abandoning or reducing the use of Internet. For many users, the second alternative is not feasible.

Despite the declared incidents and the poor knowledge of the risk shown by the users, the general feeling is that of comfortable security when using the Internet. The vast majority thinks that their connection and equipment guarantees a safe surfing. But this is not always the case.

Indicators of Electronic fraud incidents

Among the amount of indicators used to localize electronic fraud, we can first count on the Anti-Fraud Command Center Reports of RSA or those of Anti-Phishing Working Group. These reports nevertheless do not include, technically speaking, the total amount of information. We can find in them a ranking of the countries that are a target of the attacks, in which Spain has a variable presence (from the 4th to the 7th position). In March 2009, the number of fraudulent attacks in Spain was a 25% of the total. And this is because, for example, electronic banking is still one of the online uses more generalized among Spaniards. The number of online banking users in Spain has increased, in the last years, placing it in the same levels of those of the rest of the European countries. Spain was also the second one in March in number of fraudulent activities or elements.

For INTECO, performances are focused, on one hand, on the attack to Spanish entities and, on the other, on attacks using resources placed in Spain. The reports of the users are commonly used as important information sources or for the detection of new cases. Reports are more and more received as types of frauds that were, up to now, less known such as phishing.

Incidents and internet fraud

Defrauders tend to use different attacks that affect the logic security of the PC or the website such as virus, service denial attacks, data o email account robberies and identity theft through the net.

Moreover, they try to take advantage of the vulnerability found using social engineering based on current issues with a great impact. The so called “social engineering” is the specialised or empiric technique used for the studied or handy actions that allow the manipulation of people so that they voluntarily do things they wouldn’t do in normal conditions. A good example in the daily life can be the seller who makes a research on the habitudes and hobbies of the customer in order to establish the relationship between trust and empathy, to be able to sell more easily his products or services. The current economic situation provokes a bigger exploitation of fraudulent resources, but it does not necessarily provoke the apparition of new resources or techniques. The old ones are adapting to the economic, political and social reality. With the crisis and the rise of unemployment, fake and fraudulent job offers are published, opening, this way, a new concept in this technique that takes advantage of economic uncertainty.

Despite the recommendations made, it looks that phishing to financial entities is still the biggest online fraud (4 different attacks per month). Let’s remember that phishing is an attack with which any cyber criminal tries to get banking or financial information about the victim (passwords, bank account numbers, etc.). There are different ways of attacking: one of them can be sending a fake email on behalf of the bank asking for personal information with any excuse. This way, they reply or click on a link that seems to be the bank web page. They tend to be clearly planned, directed, sophisticated, dynamic and intelligent attacks..

But not only financial entities are the target of this kind of attacks. For the companies that need to transfer personal information through the Web, trust of online customers is vital. Those consumers buying online are worried by identity theft and, thereafter, they are very cautious when giving their personal information (moreover this related to the credit card) in the sites they don't know. In other kind of business, the information transferred, even though their character is not personal, is also important. This way, more and more shops, business, companies or multinationals are victims of electronic fraud or are used to commit, on its behalf and through fake Web pages with a high social engineering and conventional technique design, fraudulent activities. These frauds are made from servers located in a country different from that in which the fraud is made. Delocation used to avoid detection is quite common. It makes the monitoring process more difficult to the competent authorities.

■ **D. Julio Cortés**
European Consumer Center (Consumer National Institute)

Protection of consumer in Europe: CEC Net

he European Consumer Center is a public customer's office placed in any state member of the European Union for any need of information or assistance related to any purchase or use of a service in a country other than that of the consumer. Any cross-border transaction is observed and analysed, and mediation on any complain made is offered. The aim is getting, through a preventive and informative labour, the certainty that, in any European country, consumer rights will be recognised and granted.

The European Consumer Center in Spain will help you if::

• You are a citizen of a EU estate purchasing or contracting any service in any part of the Spanish territory

• You are a Spanish citizen purchasing or contracting any service in any EU country other than Spain

Some of the work of the European Consumer Center is to spread information about the rights of the consumers in the European Union, as well as the challenges we face due to the advance of, among others, new technologies. The increase of Internet transactions causes, unavoidably, the increase of the number of complains related to fraud. In 2007, 56% of the European complains were related to e-commerce and most of them were based on confused or inexistent terms and conditions in the contracts, delays or loss in purchases made through the Internet, etc. This has generated a high level of distrust on the part of the user: 27% of them buy through Internet on a daily basis, but 70% of them do not trust it when doing a purchase. Consumers should trust it but they do not have enough information about the possibilities of getting their money back through the methods of payment. A secure method of payment ensures the rights of the consumer.

Secure methods of payment on the Internet

The European Commission aims to remove any barrier on the cross-borders payments and to create only one payment space. But nowadays, is has been verified that, this transfers are still more expensive and slow than money transfers made in the same country because, frequently, payment systems and security rules of the different states are not always compatible. For example, being able to move the charges done back depends on the law of each country and it is demanded to prove fraud.

Problems detected since 2004 still persist today. One of them is the lack of clarity in the Web pages where methods of payment, terms and conditions of the contract or the final price of the product are not well specified. Another one, and probably one of the most important, is the lack of education of the consumers against fraud and the lack of promotion of responsible use of the methods of payment and rights of consumer. Internet consumers do not have fewer rights than those of traditional consumers. Finally, it is remarkable the need of effective mechanisms as an alternative solution for the Internet conflicts.

European cooperation projects

The European Commission aims to remove any barrier on the cross-borders payments and to create only one payment space. But nowadays, is has been verified that, this transfers are still more expensive and slow than money transfers made in the same country because, frequently, payment systems and security rules of the different states are not always compatible. For example, being able to move the charges done back depends on the law of each country and it is demanded to prove fraud.

Problems detected since 2004 still persist today. One of them is the lack of clarity in the Web pages where methods of payment, terms and conditions of the contract or the final price of the product are not well specified. Another one, and probably one of the most important, is the lack of education of the consumers against fraud and the lack of promotion of responsible use of the methods of payment and rights of consumer. Internet consumers do not have fewer rights than those of traditional consumers. Finally, it is remarkable the need of effective mechanisms as an alternative solution for the Internet conflicts.

European cooperation projects

CEC wants to use its direct knowledge of the fraud cases to bring this problem of the consumer beyond the assistance of the particular cases. In order to do so, they have established periodic meetings with the business sector held to observe the conformity with the current legislation concerning the consumer protection. This way, they will closely work with the Police and other national and international institutions in order to improve this protection through the interchange of information about bad commercial practices.

CEC organises the so-called “Día del Barrido de Internet” based on the revision of Web pages all around Europe on the problematic subjects, such as fraud in flight tickets offers. This analysis has found cases of misleading advertising and default of the legal requirements established for the Internet flight tickets sale. The research has been done together with other countries in the European Union as a reply to the initiatives of European organisms of consumer protection, always checking the compliance with the European regulation in every country and the non use of abusive concepts or non imposition of abusive conditions.

The origin of this regulation can be found in Article 51 of the Spanish Constitution where public powers are urged to guarantee the defence of consumers and users, protecting, with effective methods, their security, health and legitimate economic interests. In the same way, the General Law for the Defence of Consumers and Users Act, July 19th 1984, and the late version of November 2005, anticipated the fact that the Government should establish an arbitration system that, without any special formality, could pay attention and solve, with binding and executive character, both complains and claims made by consumers and users. Finally, the Royal Decree 636/1993, May the 3rd ruled the Consume Arbitration System and the Act 44/2006, December the 29th improves the protection of consumers and users, establishing its sixth final disposition in a year maximum after coming into force. The Government, taking into account the approval of the autonomous communities, will announce a new regulation for the Consume Arbitration System that will regulate virtual arbitration. According to this mandates, the decree is enacted. Its article 51 establishes as follows: “Electronic consume arbitration is that which is fully substantiated, from the request of the arbitration to the termination of the procedure, electronic media notifications included, without prejudice to any arbitral performance to be done by traditional means".

Article 53: “Electronic signature. Without prejudice of the use of other techniques ensuring the authenticity of the communication and the receiver identity, the use of the electronic signature ensures the authenticity of the communication, the identity of the parts and the arbitral organ".

Article 54: “Notifications will be made in the electronic address designated by the parties, being them legally made the day after the date established for the access to the contents of the arbitral performance that has been notified. But if the notified person did not have access to the contents of the arbitral performance ten days after the date and time in which it was at his disposal, the notification will be considered without legal force, proceeding to the publication of the edict in the electronic addresses of the Arbitral Commission of Consume ancillary to the electronic consume arbitration".

The future: Online troubleshooting systems

Online troubleshooting systems are product of the popularization of the media on the Internet brought by the use of electronic mail, among others, as an easy, fast and cheap method. Other tools, such as chat or messenger have allowed easy and cheap communication all over the world. On the other hand, the development of online commerce has given a big number of transactions between on-line traders and buyers, for a big or small amount of money that has generated a high number of problems to solve. Up to know there are important and new subjects that need to be studied in order to create confidence in the initial interaction between the parts, between buyers and sellers in the electronic world, when they are far away and only connected by a PC. Trust building in the trader or provider of online services is closely related to offering or not a procedure that allows the customer to talk to the entity and show his claims or complains if anything fails. Although having the customers feedback is very important, this possibility of offering a complain channel is still difficult to find in the electronic world, despite online troubleshooting systems are trendy in Europe. Future should be the electronic arbitration system, already applied in some countries such as Italy, and whose advantages include the fact that we do not have to go anywhere anymore. Defending consumers is updating and integrating information society by rights.

PART 4

Conclusions and proposals of ADICAE

CONCLUSIONS

■ During the symposium we have highlighted the worrying increase of the attacks, not only in number but also in diversity, affecting users of methods of payment in Europe every year. The main objective of these attacks is finding out personal information, moreover data related to bank accounts. Phishing and Internet are still one of the main weapons criminals use, although we shouldn't forget about cashiers or shops, where criminals still act due to the proliferation of the use of credit cards in any kind of payment.

■ The more and more complex and fast techniques used by criminals are also worrying. They show the methods they have and their ability to evolve, dominate and avoid technologic and security means companies have.

■ The main characteristic of fraud is the transnational character, because it is mainly used on the Internet.

■ We have seen the need of communication among the different police bodies in different countries that also need the help of everybody who experiences or knows about fraud. Without the report, pursuing criminals is impossible.

■ It is essential to sort out and conciliate the legislation that is not reconciled among the EU countries, not only for prevention but also for the punishment of criminal conducts related to fraud.

■ It is obvious how financial entities are not transparent when talking about fraud in the methods of payment and how they do not recognize the seriousness of the issue. According to them, they barely suffer these effects, despite statistics and data that do not say the same.

■ It is now evident who suffers fraud: the user. The user suffers all the effects. He is unprotected by the financial entity that does not recognize its own responsibility and derives it completely towards the user, who seeks for protection in the signed contract.

PROPOSALS

According to this, it is stated that measures and initiatives undertaken up to now in order to prevent and fight against fraud and counterfeit in the different methods of payment have not been enough to stop the spread of this phenomenon. Many agents are relevant in this sector of the methods of payment, and each of them is partially implied in this issue of fraud. From them, we could launch different measures that could stop this issue:

European Union States

■ Increase the resources assigned for prevention of fraud in different senses:.

- Give better security measures to the payment methods used by their customers. Use the existing means that haven't been generalised: token usb for Electronic banking, use of coordinate cards for the customers who use Electronic banking, double operations validation means (mobile phone), etc.
- Promote security culture: among the employees, through formation courses and among the customers with formative campaigns, publications, etc.

■ Engagement of revision on the part of financial control institutions (National Banks) of the payment methods contracts in order to remove abusive clauses that, nowadays, leave consumer undefended in a fraud situation.

Judiciary:

- Continuing education about this issue in judicial schools and centers of legal studies
- Cooperation and collaboration with Police and Administration bodies related to the issue

Issuers and specialized security companies.

- Fraud prevention (developing security patches that minimize vulnerabilities in the operative systems and software and giving service to financial entities with traffic filtering systems, protection against intruders, detection of fraudulent webs, etc.)
- Research and technologic innovation collaborating with other agents implied such as National Security Forces

Shops and companies working on the Internet

- Insist on security as a main aspect in business on the Internet
- Consider resources assigned to protect communication security as an investment
- Consider security as an aspect of quality service
- Formation plan for the employees in terms of security and data protection, even establishing "Security culture"

Consumers

- Bigger demand when using payment methods: Periodic update of measures and security tools (antivirus, firewalls, etc.), caution when using cash points (checking the cashier and if something weird not using it and reporting to the entity);
- Use of electronic ID card in order to validate and confirm operations made on the Internet..
- Caution. In case of running an operation and suspecting something, not doing it, in case of having done it, report it as soon as possible in the closest police station.
- Demand security to the service provider. Demand secure measures that make you trust the service.

Consumer associations

- Undertake information campaigns and spread them in order to call the attention of the user about the possible risk guidelines derived from the use of the different payment tools. This way, a responsible participation that allows a better and efficient fight against fraud can be taken.
- Collaboration with the Administration and the Police forces, not only for spreading the knowledge and experience to the associates but also for denouncing the cases.

ADICAE

al servicio de los usuarios en toda España y en Europa

SEDES DE ADICAE

Servicios Centrales ADICAE
C/ Gavín, 12 local 50001 **Zaragoza**
Tfno. 976 390060 - Fax 976 390199
aicar.adicae@adicae.net

Madrid
Embajadores, 135 1º C int.- 28045 **Madrid**
Tfno. 91 5400513 Fax 91 5390023

Catalunya
c/ Entença, 30 entlo. 1º - 08015 **Barcelona**
Tfno. 93 3425044 Fax 93 3425045

Comunidad Valenciana
Av. Pérez Galdós, 97 pta.1 - 46018 **Valencia**
Tfno. 96 3540101 Fax 96 3540106

c/ Aparicio, 5 entlo. 5 - 03003 **Alicante**
Tfno. 96 5926583

Galicia
Avda. Gral. Sanjurjo, 119 -1º dcha
15006 **A Coruña**
Tfno. 981 153969 Fax 881 927603

Castilla y León
c/ Caridad, 1 - 2ºC - 47001 **Valladolid**
Tfno/Fax. 983 373173

Extremadura
c/ Camilo José Cela, 1 3º - 06800 **Mérida**
Tfno/Fax. 924 387468

c/ Gómez Becerra, 25 3º - 10001 **Cáceres**
Tfno/Fax. 927 626336

Andalucía
Av. Eduardo Dato, 85 1ºB - 41005 **Sevilla**
Tfno/Fax. 954 652434

c/ Salvador Noriega, 7 entreplanta dcha
29006 **Málaga**
Tfno/Fax. 952 088955

... o pregunte por nuestras delegaciones en otras provincias

ANNEXE

Transposition of the Directive on Payment Services

MEMBER STATES' TRANSPOSITION PLANS

Member State	Update	Expected date for adoption	Expected date for entry into force
Belgium	An ad hoc working group consists of all competent authorities involved (relevant Ministries, NBB, Commission bancaire, financière et des assurances) has been set up. The supervisory authority (CBFA) is, in consultation with the Minister of Finance, responsible for implementing Title II, while Titles III and IV fall within the responsibility of the Ministry of Economy, in consultation with the Ministers of Finance and Consumer Protection. A draft regulation was set up end 2008, followed by mandatory opinions. Submission to Parliament in second quarter of 2009. No general public consultation has been foreseen.	3rd Quarter 2009	1 November 2009
Bulgaria	The Law on payment services and payment systems, transposing the PSD, was published in the State Gazette No 23 on 27.3.2009 and is accessible from the web page http://dv.parliament.bg/.	27.3.2009	1 November 2009
Czech Republic	Transposition work has advanced. Ministry of Finance is leading the process, but in close cooperation with Czech National Bank. The Ministry draft is nowadays being consulted by legislative committees of the government; the draft law will be submitted to Parliament by end-April 2009 and could be adopted by the Parliament in the autumn 2009.	2nd Quarter 2009	1 November 2009
Germany	The bill implementing the supervisory part of the PSD has been adopted by the Federal Parliament on 26 March 2009. It will now be transmitted again to the Federal Council for approval. Regarding the bill implementing the civil law parts of the PSD, a public hearing took place in the Federal Parliament on 23 March 2009. The bill is expected to be adopted in May/June before being retransmitted to the Federal Council. Both transposition procedures are expected be completed before the summer break.	2nd Quarter 2009	31 October 2009
Estonia	Work on draft law transposing the PSD is chaired by the Ministry of Finance. Titles III and IV are being dealt with by Ministry of Justice. The preparation of the draft is being closely consulted with the Bank of Estonia and FSA. The objective is to send the draft law for a public consultation in April 2009 and submit it for	3rd Quarter 2009	1 November 2009
Ireland	Transposition work has already commenced. The Department of Finance and the Central Bank and Financial Services Authority of Ireland are working in close cooperation with the State's legal draftspersons to finalise the transposing legislation. It is planned to carry out a concurrent consultation on the draft regulations with relevant stakeholders, including on the question of Direct Debit migration. Consultation to take place during the summer period (July, August).	3rd Quarter 2009 (September)	1 November 2009
Greece	The members of this ad hoc transposition Committee represent public authorities, regulatory authorities and the private sector. To date, the law drafting committee has met nine times and finalised the first reading of the draft law. The draft law was finalized mid-February 2009 and was consequently submitted for public consultation with all relevant stakeholders (financial institutions, consumer protection associations, chambers of commerce, etc). Two major issues still under consideration are the following: – the application of Title VI of the PSD to micro-enterprises in the same way as to consumers (Article 30, par. 2 and Article 51, par. 3) and – the mandate migration of the current legacy direct debit payment transactions.	2º Cuatrimestre 2009	1 November 2009

Spain	The Council of State has just published its mandatory report on the draft law. The Council of Ministers will send the text to the Parliament in April.	3rd Quarter 2009	1 November 2009
France	Ad hoc working group consisting of Banque de France, relevant Ministries, Banking federations, consumer groups, telecom providers, etc. already met several times. A bill aimed to authorise the Government to transpose the PSD through Ordonnance was adopted on 5 August. A public consultation was launched on 3 September 2008 and closed on 31 October 2008. The draft law will be submitted to the Council of State by April and the ordonnance is now expected to be adopted by the government before the summer.	2nd Quarter 2009	1 November 2009
Italy	Transposition work has started. An ad hoc Working Party consisting of Ministry of Economy, supervisor, NCB and banking representatives has been set up and can be expanded if need be. Parliament is expected to approve the delegation law by the end of April. The legislative decree (primary law) of transposition will be approved by the Government over the summer and, in any case, by November 2009.	3rd Quarter 2009	1 November 2009
Cyprus	The NCB was responsible for preparing the draft law. Work was carried out in close cooperation with the Ministry of Finance. Other stakeholders involved in the working group were the Co-operative Societies Supervision and Development Authority and the Competition and Consumer Protection Service of the Ministry of Commerce, Industry and Tourism. All the other stakeholders are represented in a steering committee for SEPA. A public consultation was launched on 17 December 2008 on the draft law and draft secondary legislation (a Central Bank of Cyprus Directive transposing provisions contained in Title II and Article 88) that will transpose the PSD into Cyprus law. Both drafts are available on the website of the Ministry of Finance (www.mof.gov.cy) together with an accompanying note. Comments from six stakeholders were received within the deadline (30 January 2009). Furthermore a request of the Ministry of Finance for an ECB opinion on the draft law was submitted on 5 March 2009. The aim is for the draft law to be submitted to the House of Representatives of the Republic of Cyprus already in spring 2009, allowing thus for the appropriate procedure within the House of Representatives to be followed.	4th Quarter 2009 (October)	1 November 2009
Latvia	Ministry of Finance has started implementation. No formal working group established, but close cooperation between Ministry, NCB and FSA.	3rd Quarter 2009	1 November 2009
Lithuania	Draft laws transposing Directive are currently provided for the public consultation and are available at http://www.finmin.lt/web/finmin/teises_aktai/rengiami?erp_item=rengiami_teises_aktai_000154. Public consultation will last until the end of April. It is envisaged, that draft laws will be transmitted to the Parliament in June. Adoption may take place in July.	3rd Quarter 2009 (July)	1 November 2009
Luxembourg	The draft law has been approved by the Council of government on 6 March and has been transmitted to the Parliament and the Council of State. The objective remains to have the law adopted before 1 November 2009.	3rd Quarter 2009	1 November 2009
Hungary	A special committee on political issues adopted the first draft Act on Payment Services, which will be the main instrument for transposing the PSD (besides secondary legislation: a Government degree and a degree of the NCB) on 12 December. This draft was available for consultation through the website of the Ministry (http://www1.pm.gov.hu/) between 19 December and 9 January. Submission to the Parliament is foreseen for early April.	2nd Quarter 2009	1 November 2009

Malta	NCB has the lead for transposition and cooperates closely with Malta Financial Services Authority (MFSA, responsible for Title II) and the Office for Fair Competition. Following the publication of a consultative document and an extensive public consultation process, the Central Bank of Malta (CBM) has published a summary of responses received (available at www.centralbankmalta.org), and a joint MFSA/CBM committee is now preparing draft legal amendments taking into account the outcome of that process and PSDTG conclusions. While it is envisaged that much of the PSD will be carried into effect by means of subsidiary legislation issued by the MFSA and the CBM under the Financial Institutions Act and Central Bank of Malta Act respectively, a Bill to carry out certain amendments to these acts will be placed before Parliament probably by end-April.	2nd Quarter 2009	1 November 2009
Netherlands	The Dutch ministry of Finance has written a draft amendment of the Financial Supervision Act and the Civil Law. Last summer stakeholders have been consulted on the draft. The bill has been sent to the parliament. The Second Chamber will probably deal with this bill before summer; the First Chamber probably deals with this bill in the third Quarter of the year. A consultation on the secondary legislation will take place during the second Quarter 2009.	3rd Quarter 2009	1 November 2009
Austria	The draft law has been sent out for formal consultation in January 2009 (https://www.bmf.gv.at/Finanzmarkt/RechtlicheGrundlage_753/Zahlungsdienstegesetz/_start.htm); the consultation was open until end February. Submission of final draft to Parliament after Easter.	2nd Quarter 2009	1 November 2009
Poland	The public consultation regarding the PSD implementation act will be launched in April.	2nd Quarter 2009	1 November 2009
Portugal	A first draft has already been delivered to the Ministry of Finance and has been submitted to consultation. The public consultation has been finalized and the Ministry of Finance will soon receive a final proposal that will be assessed and by the end of that process submitted to the approval of the Government.	3rd Quarter 2009	1 November 2009
Romania		3rd Quarter 2009	1 November 2009
Slovenia	The text of the legislative proposal implementing the Directive, prepared by Banka Slovenije, was submitted by the Slovenian Ministry of Finance into consultation to different stakeholders on 16 December 2008, for comments until 9 January 2009. A draft law should be submitted to the Government by April 2009.	3rd Quarter 2009	1 November 2009
Slovakia	The draft legislation transposing the PSD (in Slovak language) is now publicly available through 'comments proceeding' on the website of the Ministry of Finance of the Slovak Republic at http://www.finance.gov.sk/Default.aspx?CatID=7209 and also on the Legislation Portal of the Ministry of Justice of the Slovak Republic at https://lt.justice.gov.sk/(X(1)S(2twtim45suofcnf02gawma2m))/Material/MaterialHome.aspx?instEID=- 1&matEID=1267&langEID=1.	2nd Quarter 2009	1 November 2009
Finland	Two working groups were set up: one with Ministry of Justice (work on Titles III and IV), one with Ministry of Finance (rest of PSD); all relevant stakeholders are represented (including Telco's and consumers). The draft bill prepared by the Ministry of Justice is available in the official website of the Ministry. The draft bill to be prepared by the Ministry of Finance should be available by mid-May. The official consultations of both draft bills should take place in early summer. The draft laws should be submitted to Parliament by October 2009.	4th Quarter 2009	1 November 2009

Sweden	There is a risk that Sweden will not be able to implement the Directive until 1 November. According to the revised timetable it is intended to put forward a proposal to the Parliament in December.	?	?
United Kingdom	The Regulations implementing the EU Payment Services Directive into UK legislation entered into force on 2 March 2009. A summary of responses to the consultation on the draft legislation, together with an explanatory memorandum to the regulations was published on 12 February 2009. These documents can be found at http://www.hm-treasury.gov.uk/fin_payment_index.htm. The FSA published a consultation on its rules to implement out-of-court complaint and redress procedures in August 2008 and expects to publish the final rules in March 2009. As for the territorial scope of the adopted measures, it is still under consideration whether further legislation would be required for Gibraltar and the Channel Islands. The FSA has been published its Approach Document, Perimeter Guidance and Policy Statement to help firms understand the Directive's requirements, and what they need to do to prepare for November. There available at http://www.fsa.gov.uk/Pages/About/What/International/psd/.	2 March 2009	Full implementation (PSPs must comply with prudential and COB requirements): 1 November 2009 Information sharing and cooperation with other authorities: 2 March 2009 Firms can start making applications: 1 May 2009

EEA COUNTRIES

Iceland	A draft bill implementing the PSD 2007/64/EC is not available yet.	3rd or 4th Quarter 2009	1 November 2009
Liechtenstein	Formal draft during 3rd Quarter 2008, final draft during 2nd Quarter 2009.	3rd Quarter 2009	1 November 2009
Norway	The special transposition working group with representatives from the relevant ministries, the NCB (chair), the FSA, consumers and industry delivered their first report on Titles III and IV in February 2009, and a public hearing has been held. The report and the response can be found at http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2009/horing---forslag-til-gjennomforing-avbe. html?id=546595. The Ministry of Justice will propose amendments in the Financial Contracts Act as a transposition of Titles III and IV shortly. The Norwegian Parliament will probably review the bill before it breaks for summer. The working group plans to deliver a report on Title II to the Ministry of Finance later in the spring of 2009.	2nd Quarter 2009	1 November 2009

Fuente: Comisión Europea, DG Internal Market, http://ec.europa.eu/internal_market/payments/framework/transposition_en.htm