INTERNATIONAL PROJECT ADICAE

European cycle of Seminars against the fraud in means of payment

The fraud to discussion between European consumers

Conclusions and offers of the seminars celebrated in the whole Europe

Organises:

ADICAE
Association of Users Banks, Savings Banks and Insurances

With the collaboration of:

DG JUSTICE, FREEDOM AND SECURITY
European Commision

Edits:

ADICAE
Association of Users of Banks, Savings Banks and Insurances

Central Office

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

A-S 200107

Index

PART 1 - A PROJECT FOR ALL THE MEANS OF PAYMENT CONSUMERS

PART 2 - EXPERIENCE OF THE EUROPEAN COUNTRIES IN THE FIGHT AGAINST FRAUD

PART 3 - CONCLUSIONS AND PROPOSALS FROM ADICAE

PART 1

A Project for all the means of payment consumers

Book presentation

BOOK PRESENTATION

Nowadays, and increasingly, it is indisputable the progress in the use of tools that enable consumers to pay for their purchases of goods and services without using any bank notes or coins, ie, the means of payment other than cash.

Cards, transfers, checks, electronic banking, payment through mobile phones and many other tools are available to almost all consumers and its market has increased dramatically in recent years. Just as an example, in the euro area there are currently over 350 million cards in circulation which as a whole are used in more than 12,000 million payment transactions. Cards, transfers, checks, electronic banking, payment through mobile phones and many other tools are available to almost all consumers and its market has increased dramatically in recent years. Just as an example, in the euro area there are currently over 350 million cards in circulation which as a whole are used in more than 12,000 million payment transactions.

If global progress of the different means of payment seems exorbitant it is more remarkable the progress of its frauds. Los fraudes en los medios de pago distintos al efectivo son delitos de índole económico cometidos generalmente por bandas organizadas que se basan en la violación de los mecanismos de seguridad de estos instrumentos para así disponer de la capacidad de usarlo en beneficio propioen perjuicio del consumidor, que en numerosas ocasiones El uso de códigos maliciosos y programas informáticos especializados en el robo de información está proliferando de manera preocupante, al igual que las bandas organizadas que tienen sus redes extendidas por todo el mundo y que hacen de estos fraudes y otros delitos su medio de vida. Fraud in the means of payment other than cash are economic crimes usually committed by organized gangs that are based on the violation of the security mechanisms of these instruments and have the ability to use it for personal gain and against the consumer. The use of malicious codes and software specialized in information theft is proliferating in a preoccupying way, the same as the organized gangs that have spread their networks across the world making a living out of these frauds and other crimes.

ADICAE, the only spanish consumer organization specialized in Banks, Cash & Insurance, concerned about the situation of vulnerability in which users of these means of payment are has led the international project "European cycle of seminars for the prevention of fraud in the means of payment in conjunction with law and judicial enforcement, consumer associations and professional organizations funded by the General Directorate of Justice, Freedom and Security of the European Commission in which collaborates with other 8 european consumer associations. ADICAE y las demás asociaciones de consumidores celebraron diversos Seminarios en los diferentes países en los que se llevó a cabo el Proyecto. ADICAE and the rest of consumer groups held several seminars in different countries that carried out the project.

The aim of this publication is to report on the seminars that took place throughout Europe in the framework of this project in various countries posing an interesting debate between different actors in the sector (financial institutions, card providers , ATMs or readers, computer security companies, law enforcement, regulatory, management, etc) to get to put in place mechanisms to ensure consumer protection and ensure that progress and security go hand in hand. We can say that another major objective of the project organized by ADICAE is to inform users of risks to prevent the use of these instruments of payment, and that throughout our long experience in the field of consumer protection we have observed each time major problems in knowledge about the use of means of payment and disputes arising between consumers and financial institutions in their relationship as a supplier and user of means of payment.

We believe that this publication from ADICAE, as the rest of the project, are an extremely useful tool for both users and academics such as academic, technical, consumer, law enforcement and general practitioners interested in issues of consumption, electronic commerce and payment instruments other than cash.

PARTNER ASSOCIATIONS

ADICAE

Association of Users of Banks, Savings Banks and Insurances of Spain

Bulgary: "National Bulgarian Association of Consumers (BNAP)"

Slovak Republic: "Slovak Consumer Association (ASC)"

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

Lithuania: "Lithuanian National Consumer Federation (LNCF)"

Czech Republic: "Sdružení českých spotřebitelů (SČS)"

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

PUBLICATIONS OF THE PROJECT

Juridic Study of Fraud

Book of the Project International Seminar

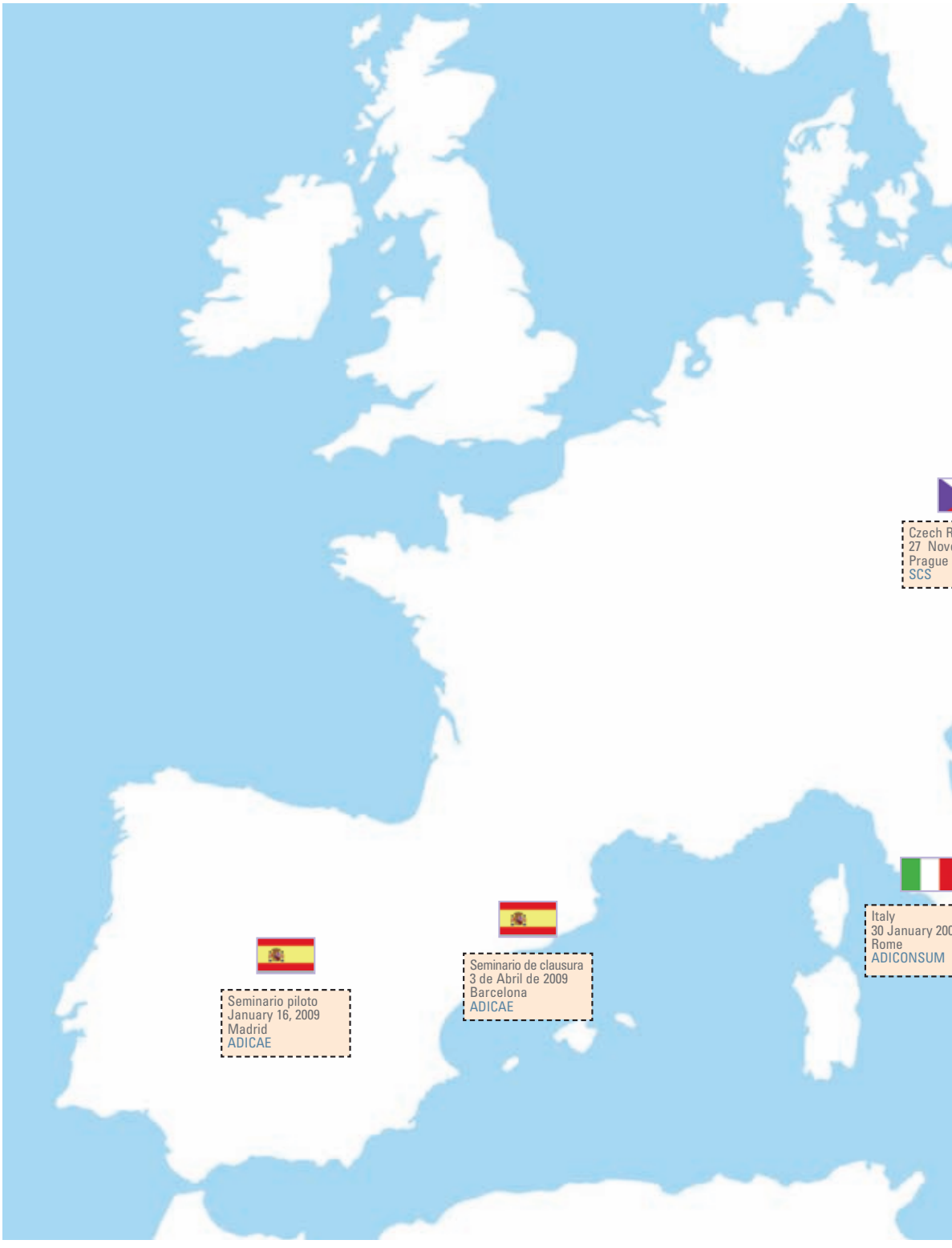
Web page of the Project

Electronic Simulator of Fraud

PART 2

Experience of the European countries in the fight against fraud

Partner Countries Seminaries


Seminario piloto
January 16, 2009
Madrid
ADICAE
Seminario de clausura
3 de Abril de 2009
Barcelona
ADICAE
Italy
30 January 200
Rome
ADICONSUM


Lithuania
16 December 2008
Vilnius
LNCF
epublic
ember 2008
Slovak Republic
7 April 2009
Bratislava
ZSS
Romania
23 March 2009
Bucharest
ANPCPPSR
Bulgary
28 January 2009
Sofía
BNAP
09
Italy
13 February 2009
Rome
MDC

"FRAUD ON THE MEANS OF PAYMENT: THE GREAT CHALLENGE FOR EUROPEAN CONSUMERS"

- Organised by ADICAE
- January 16, 2009
- Convention Hotel, Madrid.

Speakers:

D. Emilio Vicente Quintano,
Chief Inspector of the National Police Corps, head of the Means of Payment and appointed by the General Directorate of Police and the Guardia Civil for collaboration with ADICAE.

Javier Berciano Alonso,
Area Coordinator - Facilities and Operations Reagents INTECO-CERT (Institute of Communication Technologies went eConfianza / Programs Directorate. Replaced Elena Garcia, the contact of INTECO ADICAE. INTECO Institute is an official of the Ministry of Industry which remains very active in such matters.

D. Javier Díaz Martín,
Director of Business MOBIPAY. MobiPay es una empresa que gestional la logística y la seguridad del pago por móvil, servicio ofrecido por algunas entidades financieras como BBVA, Santander, Caja Madrid, Banesto y Banco Popular. MOBIPAY is a company that gestional logistics and security of mobile payment service offered by some financial institutions such as BBVA, Santander, Caja Madrid, Banesto and Banco Popular.

PRESENTATION OF RESULTS OF THE STUDY ON FRAUD CARRIED OUT BY ADICAE

As a starting point for the celebration of various national and international seminars, a study with several parts (legal, sociological, statistical) was elaborated, making an strict analysis of the phenomenon of a huge proliferation which is fraud and its causes. The result is that technical and judicial issues had much weight (which are discussed in this publication) specially legal regulations, unfair terms and the resolution of complaints from users.

In an initial analysis it was identified that the common prejudices suffered by users victims of fraud through various mechanisms, were as follows: charges for non-made purchases (in person and online), Electronic Banking fraudulent transfers by deception and extortion from third countries, in addition to the substitution of personality.

The ADICAE study analyzed basically three types of contracts: credit and debit cards (both in its use as a face on the Internet), electronic banking and other means of payment (transfers, direct debit, mobile payments and checks). 39 different types of contracts of means of payment were analyzed belonging to 20 major financial institutions that sold in Spain.

Some of the organizations studied were-BANCO SANTANDER CENTRAL HISPANO, BBVA, Barclays, Citibank, BANCO CAIXA GERAL, BANESTO, OPENBANK, Cajasol, Caixa Galicia, Ibercaja, CAJA POPULAR LABORAL, LA CAIXA, Caixa Cataluña, INMACULADA BOX, Caja Vital Kutxa , Caja España, Caja DUERO, CAJA RURAL DEL SUR.

The problemas of the improper clauses

It is clear that unfair contract terms of payment exist and will continue to exist and, which contravene both Recommendations (non-binding legislation at European level) as codes of good behaviour adopted by the industry. Therefore it follows, contrary to what the financial institutions claim on that self-regulation and "soft" are not real solutions to this problem, but only serve to prolong the situation of helplessness of the consumer. Financial institutions do not respect even basic rules of game, set by themselves

Referring to unfair terms, one of the main factors that enable their existence, thus legitimizing bad practices of financial institutions is the shortage of financial education (which on the other hand, do little or nothing to improve the entities); through the profound experience of ADICAE there is evidence that consumers don´t generally read the contract thoroughly and understand exactly what they are signing, and therefore what their commitment is. Also we have seen no Control of adhesion contracts in services offered by financial institutions, primarily by its regulator (Bank of Spain), in addition to contravening the Act on General Terms and Conditions, leaving them in a register regulated by the Ministry of Justice . Finally, it is remarkable the lack of ways to prevent marketing contracts with this kind of clauses that undermine the rights of users.

As first steps, so that the user could protect himself from this abusive situation established by financial institutions, we would highlight the collective bargaining prior to the removal of unfair terms, the hiring of additional security mechanisms by institutions to reduce the phenomenon of fraud, the comparison between the different terms offered by financial institutions, in addition to the application of professional and independent advice to a Consumers' Association at any time (before or after) of recruitment.

In the worst case, once it has suffered the injury financial institutions should be applied through the extrajudicial system for resolving conflicts, which claim to the Bank of Spain if a claim is not satisfactorily resolved by the Service Customer Entity, but this system has many flaws and shortcomings as it has been denouncing ADICAE for many years.

ADICAE EXPERIENCE IN THE FIGHT AGAINST FRAUD

Knowing the reality of ADICAE shows that it is vital to guarantee the basic rights of users to the means of payment fraud. Éstos suponen indudables beneficios y comodidades para los consumidores aunque sólo en el caso de ser bien entendidos y utilizados. They pose obvious benefits and convenience to consumers but only if it is well understood and used. The frauds in the means of payment get to about 4122 billion Euros a year, which makes even the police be overwhelmed and overtaken by declaring these scams.

One of the main objectives of the Project is to create a common dialogue between the different actors involved in this problem, especially means of payment providers, banks, police, judiciary, security companies and institutions.

At present, it is worth noting that in terms of consumer protection in the topic of means of payment fraud in the existing regulation the main recommendation is that of 30 July 1997: restricts the user's responsibility in the first € 150 if fraud, except for a negligence in the custody or use of the card. Also notable is the inadequacy (if not absence) regulations for Electronic Banking, as we can say that the legislation is favorable to the entities.

However, we can glimpse some improvements in the legislation that will soon be adopted, as it is the case of the Directive means of payment (2007), currently being in transposition, which states that entities are the ones who must prove the absence diligence in the use of credit card. We highlight the main negative point regarding the uncertainty about consumer protection in the new means of payment that may arise in the future.

The new issue of means of payment fraud

In the past, the frauds were perpetrated by hackers who were operating normally on their own without interacting with other criminals, often without financial motivation, but at present the means of payment fraud is perpetrated by very hierarchical criminal gangs, that try to make profit and invest the one obteined out of their activitity on issues such as terrorism, drug dealing and weapons, etc..

Fraud in means of payment is currently not targeted at certain points as before, but is being committed in transnational or even transcontinental level (ie, the stolen data in a given country and the card was cloned in a different country) . Therefore, it is considered that the fight against fraud should be carried out on a transnational level and with the cooperation of all those concerned.

European initiatives in the fight against fraud

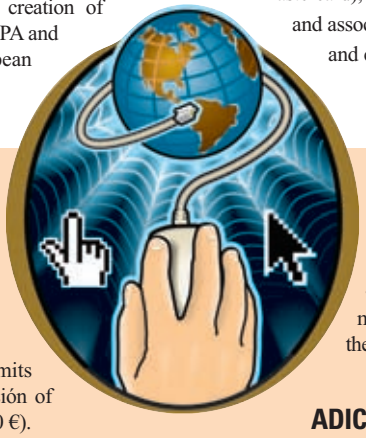
Regarding the initiatives taken at European level regarding the fight against fraud, it is important to include a variety of issues: the existence of a big diversity in legislation at European level (already mentioned), cooperation between police of different countries through Europol, the creation of various advisory groups, the develop of SEPA and action plans undertaken by the European Commission (notably the Action Plan 2004-2007)

Specifically, the priorities of the Action Plan for the Prevention of Fraud by the European Commission are:

1. The safety of products and payment systems.
2. Cooperation between government and the private sector.
3. The integration of new member states in the new framework for the prevention of fraud in the European Union
4. Closer ties with neighboring countries to the European Union concerning the situation of fraud .

It can be seen that the initiative undertaken by ADICAE is especially suited to the proyect of ADICAE.

ADICAE has extensive experience in actions to combat fraud. Since ECCG (European Consultative Consumer Group), subgroup FSCG (Croup Consumer Financial Services). ADICAE also participates in the FPEG (Expert Group on the Prevention of Fraud) providers of payment (VISA, Mastercard), European Commission, national institutions, and associations of banks, means of payment industry and consumer associations.



ADICAE has detected that the users have many means of payment disputes with financial institutions providing these services. It can be divided into two main categories:

UNFAIR TERMS

- No inclcusión of liability limits (Recommendation 150 €) No inlcusión of liability limits (Recommendation 150 €).
- Burden of proof moved to the consumer.
- Presumption of guilt of the user.

BAD BANKING PRACTICES

- Failure to comply with the judgments of the Bank of Spain in this respect .
- Delayed migration to EMV Chip-schema.
- Non-optimal Security systems.
- Consumer Associations not taken in account despite of being the authorized representatives.

Therefore, conclusions of that which has been exposed are the following:

■ Must be found to the problem of fraud:

- Financial institutions need to bet on the aim of putting an end to this issue, as one of the actors most involved in it.
- Consumers should have access to real tools for their effective protection, and join an association of consumers to ensure their rights and carry out an effective defense in this matter
- There can be no true development of means of payment other than cash without the confidence of consumers.

ADICAE tips to avoid fraud

ADICAE offers a number of tips that can help people to prevent any fraud.

- Distrust promises of easy money.
- Avoid to access e-banking services from public computers.
- Check your computer regularly.
- Check occasionally the account associated with the regular card.
- Be careful with clicking on links or downloading unknown programs.
- N ew password to access the bank: Change your passwords regularly.
- F ilter messages from strangers.
- I dentify the partner or service provider.
- A ssure when making a transaction card or bank details of the certificate of the company

COMBATING FRAUD BY GOVERNMENT OF SPAIN

The experience of INTECO

The National Institute of Communication Technologies (INTECO), organism promoted by the Ministry of Industry, Tourism and Trade, is a platform for the development of the Knowledge Society, addressed to citizens and Small and Medium enterprises through projects in the field of innovation and technology. INTECO has two main objectives: to contribute to the convergence of Spain with Europe in the Information Society and promote regional development, rooting a project in Leon with global aims. INTECO develops, among others, technology security initiatives, accessibility and inclusion in society and digital communication solutions for individuals and businesses.

The Institute carries out different programs:

Security

- Incident Response Center in Computer Information Technology for SMEs and Citizens.

- Observatory on Security of Information: The main task is to analyze, describe, advise and disseminate the culture of safety and trust in the Information Society.

- Center Demonstrator enhancer and Security for SMEs

Accessibility

It aims to ensure the right of citizens and businesses to interact electronically with the AAPP:

- Reference Center on Accessibility and Web Standards: main mission is to promote the construction techniques of Web sites on Public Administration, taking into account requirements of accessibility, ease of use and adoption of standards for construction.

New forms of fraud on credit cards

ATM

The thief gets to see the PIN that the user types, using subsequently stealing his card.

Cash handling devices in the slot machine and a micro-camera hidden: inserting the card into the reader's cashier records the card details and PIN when you dial the numbers being recorded by the micro-camera.

Locking the card inside the cash point, a stranger tells you to re-enter the PIN. Este lo memoriza y lo utiliza después con la tarjeta todavía bloqueada. This is stored and then used with the card still locked.

Telephone:

When we receive a call offering something and we are asked fou our card information.

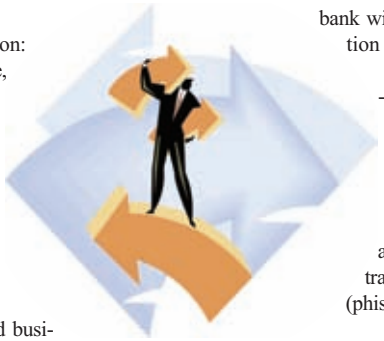
Posing as the issuer of the card and asking for some confirmation.

Of another entity, offering a bid, they need to transfer the funds to the new card.

We are reported that we have won a prize and they need to recover our data delivery costs.

The rise of internet fraud

- "Phishing": false or supplanted financial institution or trade: we make a purchase on a site that seems to be a trade, but is actually a bait to get our details or supposedly receive an email from our financial institution (fraudulent impersonation) for our data (passwords, card numbers, pins, ...). A bank will NEVER ask for our e-mail identification data.



- When making a transaction in a shop and tafter we receive non pre-authorized charges (eg subscriptions to specific services)

- False or spoofed-Commerce: We make a purchase on a web which appears to be a trade, but is actually a bait to get to our data (phishing).

- Fraud-auctions: the auction-related scams have become the most common type of fraud on the Internet, representing 42% of all complaints received by the Internet Fraud Unit of the National Consumers League of the USA . in recent years. Los fraudes de subastas se producen en los casos en los que un artículo que ha ganado en una subasta en línea no le llega nunca, o bien cuando sus características se han falseado de forma significativa. Auction fraud occurs in cases where an item we have won in an online auction never arrives, or if their features heve been distorted significantly.

- Items not delivered: consumers simply do not receive the items they have purchased online. Después de los fraudes en las subastas, éste es el segundo tipo más común de estafa en línea. After the fraud at auction, this is the second most common type of online scam.

- Financial false offers: it is very likely you have already received messages from spam con este tipo de propuestas. spam with such proposals. One person, perhaps Nigeria, is in contact with you because, apparently, is the heir of an economically significant amount. All you have to do is

provide your bank account and pay a small fee.

- Counterfeit checks to purchase goods or services in this case, the fraudster buys a product or a service, sends the seller a check for an amount higher than the price and asks him to do a transfer for value of the money left over. The original check is rejected and the seller not only doesn´t get the without payment, but also loses the money they sent in the transfer.

- Work plans at home and pyramid schemes: in these schemes large amounts of money for work done in your own home or if you get more distributors for a given product are promised. In return, the victim pays for the kits of work that will never get, or buys large quantities of a product that nobody wants, or investing in a pyramid that crumbles before receiving any compensation. In all cases, the disbursement of money is beyond the benefit obtained.

- False loans or payment of a fee to obtain credits: often based on spam messages, they are false promises of loans, especially to help some consumers to pay their debts or improve their credit. In these scams, the lender requests a fee to cover costs of loan application and then disappears.

- Fraud-related charities: they usually occur when natural disasters and other tragedies, some tricksters impersonate legitimate charities in emails and websites to get money from well-intentioned donors.

The new phenomenon of online investing

Remote banking and more Se ha generalizado en los últimos años la banca a distancia y más aún, las entidades que sólo operan por internet. has become widespread in recent years and even more organizations that only operate over the Internet. Some organizations only serve as savings accounts and do not accept debit services as common as the copper does allow other operations (transfers, have ATM cards, etc.).

Consumer Precauciones with online financial services

- Upgrading the software on our computer regularly, periodically checking the security level with which you are connected (perto scan, antivirus, firewall, sensitive data in the account setup ...).

- Performing regular backups of your data.

- Entering information could lead hazards, such as our account number, only when the page you requested is secure. (por ejemplo aquellas que empiecen por “https”.) y encriptar los mensajes y ficheros más importantes. (Eg those that begin with "https.") And by encrypting the most important messages and files.

ADICAE tips to avoid scams

In dealing with products, services, investment opportunities and donations on the Internet, the watchword is caution. The tips below can help you identify and avoid some of the most common scams on the Internet:

- Do not send money to businesses or organizations that you do not trust or whose accuracy can not be checked.

- Go to the consumer protection agency of your city and check into the office of good business practice to verify that there is no complaint about an organization that is unknown.

- Confirm the assumed contact information of organizations with which you are not familiarized, such as physical addresses, phone numbers and business addresses. Do not set any business contact with organizations that fail to provide the information without any restrictions.

- Make sure you understand all the rules of an auction before participating in it. Before you bid on an item, do everything in your power to confirm the history and contact details to the seller at the auction.

- Do not purchase collector's pieces or unique items in Internet auctions. If you can not discuss the article in advance, how can you be sure it's authentic?

- Do not send cash or make transfers to purchase goods or services online or by auction.

- Insist on receiving a receipt for the exact value of the goods or services sold over the Internet. Do not enter a check that has never received a value higher than the price negotiated.

- Even if you know the charity to confirm your request by phone online before you make a donation.

- Use common sense when responding to offers for easy money. If it seems too good to be true, it is most likely to be a scam.

- Be extremely careful if you receive unsolicited requests for payment of sums of money in advance from assumed lenders, government agencies or other organizations.

- Make all online transactions with credit cards on secure Web sites. Even if you have taken all precautions and have decided to conduct a business with a person, there is no reason that prevents you from using the safest method of payment

PAYMENTS THROUGH MOBILE PHONE

The proposal of Mobipay

Mobipay system seeks to resolve many of the shortcomings in terms of operability and safety of other ways to pay without using coins and bills and using the payment via the mobile. MOBIPAY España SA is the standard platform for payments and other safe transactions via mobile phone.

Features and Typology

MOBIPAY allows to activate a mobile phone through different financial ways of payment (Visa, Mastercard, ...) as well as to activate payments against the account of the mobile phone, transforming it into a transactional channel for conducting all types of remote payments.

How do mobile payments work?

- The consumer is associated with a mobile phone "wallet" in which you can activate a number of different means of payment from issuers.

- For each transaction, the user can choose to pay with any means of payment that are enabled in his portfolio and are admittedin the establishment.

- There is an "personal authorization key" (PIN) for every payment that is managed by the issuing entity:

- It is only known by the owner. .

- The user authorizes a transaction by entering the PIN or code indicated in each case the issuer of the means of payment being equivalent to a handwritten signature.

At present the operation of services on offer is: Payment for purchases (remote and local), transfer of funds, consults, etc..

Great unknowns and problems with security

Issues of functionality in the case that the consumer loses coverage or the phone's battery as it would prevent the user form performing the transaction due to the problems this would bring.

In case of physical theft of mobile would it be any problem to cancel the service?

The entity does not clear up the result of the consumer having a virus on the mobile phone or the signal being received by another terminal.

CZECH REPUBLIC SEMINAR

- Organised by SCS, Czech Consimer Association
- Prague, 27 November 2008
- Hotel Beránek, Václav room (Belehradska Street, 110)

Sdružení českých spotřebitelů (SČS). The Czech Consumer Association, founded in 1990, stablished as its priority the development of activities related to a preventive point of view in order to assist the consumers with the necessary tools for its protection. These activities have as its main objective to improve the relationship among services providers and consumers, trying to contribute and support the development of free markets in addition to effective mechanisms for the protection of consumers.

PROGRAMME:

10:00 OPENING Libor Dupal, President Sdružení českých spotřebitelů, Czech Consumer Association

10:15 ROUND TABLE: SITUATION OF THE MEANS OF PAYMENTS AND ITS FRAUDS IN THE CZECH REPUBLIC
František Klufa, Financial Arbiter
Libor Dupal, President Sdružení českých spotřebitelů, Czech Consumer Association

11:00 ROUND TABLE: OPINIONS OF STAKEHOLDERS(I)
Jiří Beran, Ministry of Finance and Economy
Michal Hradecký, Police HQ of the Czech Republic;
Karel Kuchařík, Police HQ of the Czech Republic;
Michaela Kolzová, Advocates' Association of the Czech Republic

12:00 ROUND TABLE: OPINIONS OF STAKEHOLDERS(I)
David Pikálek, Responsible of Security of the e-Banking Service, "Česká Spořitelna" Savings Bank
Ladislav Pauker, Representatice of teh Czech Bank Association
Karel Kadlčák, President of the Security Committee of the Association for Bank Cards
Hanka Michovská, Representative of the Asociation of de Electronical Goods Consumption

13:00 ROUND TABLE:
Speakers from the aforementioned round tables and attendants to the Seminar

ATTENDANTS: Over 40 people in total; with representatives of the Police, diverse Ministries, Banking sector (Czech Banks Association, Česká spořitelna) representatives of companies (Czech Confederation of Torism and Trade, Local Trade Office in Brno), representatives of institutions in the consumption area ((State Agency for the Inspection of Consumption-Brno, financial advisers, etc). Labor unions (ČMKOS), representatives of Universities.

DIFUSSION: There were attendind journalists from the media, such as TV channels TV1 and TVZ1, where MR. Dupal and Mr Klufa did interviews in order to disseminate the contents of the Project. In addition of this, a press review was issued.

Statistical information CZECH R.

■ Increased access to Internet users Czechs has been enormous in recent years, as it rose from 29% of households connected to Internet Czech Republic in 2006 to 46% of them in 2008.

■ If we look at the progress of broadband in the Czech Republic, we can see that it is also notable: a move from 17% in 2006 to 36% in 2008.

■ The main activities for which the Czechs users connect to the Internet si to find news and read newspapers online (33% of users) and to book trips and accommodation (26%). The activity that intereststhe least them among is the search for work and sending job applications, since only 5% of Czech users use this resource.

LEGISLATIVE STATE OF FRAUD IN THE MEANS OF PAYMENT IN CZECH REPUBLIC

The transposition of the Directive on the Means of Payment

The Payment Services Directive 2007/64/EC was adopted in late 2007 (although its design has been developed over several years). Its aim is to harmonize the regulation of payment services in the EU. It consists of a part on a more public provisions (provisions for access to the delivery of these services by businesses) and a part of a more private character (eg, concerning the mutual rights of the providers of media payment and users).This directive is the result of a complicated mutual negotiation between the various parties (and respecting the national discretion of Memeber States) Under the principle of full harmonization (Article 86 of this Directive), Member States can not amend Directive (moderatedly or strictly)

Timetable for Implementation in the Czech Republic

- Spring 08: Consultation with the various social and economic agents
- October 2008: Start preparing the text
- November-December 2008: Period of Arguments
- January-February 2009: Draft submitted to the Legislative Council and the Committee on Government
- March 2009: Draft Government sent
- April-June 2009: Vote by the House of Representatives
- August 2009: Approval by the Senate, President of the Republic

Law draft on Payment Systems: A challenge for financial institutions and issuers of means of payment

The new Law on Payment Systems involves transposing the European Directive on Payment Services, and therefore the regulation of e-money issuance and management of payment systems by private companies.

6 Highlights of the 146 sections:

- General Provisions (Common, transitional and final provisions).
- Payment systems .
- Rights and obligations for the provision of payment systems .
- Private companies-Section (Part III and IV of the Directive) .
- The administrative violations .
- Common, transitional and final dispositions.

As to the general provisions laid down by the Directive, it should be noted that you can define payment services (in accordance with the Annex to the Directive) as:

- Payment transactions (deposits, withdrawals, transfers)
- Remittances
- Issuing and administering means of payment.
- Distant payments by instrument .

In terms of scope, we believe that all transactions are carried out by a means of payment other than cash, which are:

- Directly from the payer to the payee.
- Transfer funds.
- Documents of payment instruments (checks, invoices, receipts and shipping) .

These provisions also set out who can provide payment services: banks, credit unions, e-money institutions, suppliers of means of payment for small-scale postal licensees and Czech National Bank.

In accordance with Article 26 of the Directive, providers of small means of payment: :

- You can provide payment of up to € 3 million / month
- Natural or legal persons on the basis of the inscription on the Czech National Bank (which allows simplified procedure)).

It should be noted Article 81 of the Directive, which sets as supervisor of service providers means of payment to Czech National Bank

It also appears various administrative violations established by the new law with penalties for failure to comply with the requirements established by this legislation.

New legislation relating to unauthorized transactions

The transposition of the Payment Services Directive provides relevant considerations with respect to unauthorized transactions, dividing responsibilities between the payer and the provider of means of payment.

The transaction is authorized if it has the consent of the originator – it must be submitted the form or proof of consent. If the supplier is responsible for the loss, he will be obligued to refund the amount that the payer has lost or credited to an account owned by the payer. This commitment is required immediately.

The extent of liability for the supplier is graduated, depending on whether the taxpayer has a certain amount of guilt with respect to unauthorized payment transaction.

We must remember that European legislation already exists (although not binding), which states that unless the payer is fully accountable before the loss, theft, etc.. only the first 150 Euros of the loss belong to him. After notification of loss, theft, etc. It belongs completely to the provider, except in cases of deception by the payer as we have said.

The law draft contains an important provision: using a means of payment (credit cards and others) that has logged the transaction a provider does not necessarily mean that the operation was authorized by the payer or who has acted fraudulently; or who willfully or through gross negligence, or violation of any of its obligations regarding the payment. At the same time, in case of disputes shall apply here the principle of free evaluation of evidence by a court, under the Section 132 of Civil Procedure.

Referring to the burden of proof is required for the provider to provide the documents if the user claims to the payment transaction, as it has been approved or applied improperly.

The essence of this requirement is proof of certain facts (verified, properly registered, regardless of technical failures), but it is not, however, the traditional burden of proof in terms of procedural law.

The difference with the traditional burden of proof is that if the provider fails to meet its obligation, only for this reason he would not lose any dispute, for example, but could be directly liable for damages. WeNo nos encontramos ante una transferencia automática de la carga de la prueba. do not have an automatic transfer of the burden of proof.

The reason for this is that the user is unable to prove these material facts to which they can defend themselves, contrary to what is commonly in the means of payment contracts (unfair).

THE VISION OF INDUSTRY AND PRIVATE INSTITUTIONS:

First steps of financial institutions in the Czech Republic in the fight against fraud in means of payment.

Česká spořitelna, the largest savings bank in the Czech Republic (and in many other countries of Eastern Europe) has developed mechanisms to protect their customers against fraud in the means of payment. There was a significant increase in protection of their customers for the additional security measures it has introduced in recent years, such as 3D Secure technology. Also the cooperation with business security antivirus vendors to find ways to block spam effectively has been another of the strategies carried out by the financial institution.

Another policy has been changing banking practices to achieve greater customer protection. Previously, there were transactions that did not need permission, but now are needed. For other transactions in the past was only necessary an authorization code from a client (eg to change the implementation of SMS alerts), but it is now necessary to arrive at the branch in order to configure this service.

The Czech Savings Bank operates primarily in Eastern Europe. More than 1.2 million customers use the direct banking (Internet, mobile phone or other electronic means) of the Czech Savings Bank, it has several options for customers to operate their account in person at the branch - - via phone, Internet, ATMs and mobile phones. Principal channels of direct banking of the Czech Savings Bank-SERVIS 24 - include Internet, telephone and GSM. Customers of this bank are mostly individual clients, small and medium enterprises, municipalities and large corporations;

CONCLUSIONS

- Despite some existing forums for discussions on this issue, as a Safety Commission, in which the main operating entities operating in the Czech Republic it is still necessary a greater cooperation between various actors, including dialogue with representatives of consumer associations, until now excluded from that process.

- Thanks to the new European regulations, in Czech Republic in addition tothe rest of Europe the problem of burden of proof in fraud cases means of payment seems to be being solved. It is established by the Directive on Media payment, the provider's obligation to provide the documents if the user claims to the payment transaction, as it has been approved or applied improperly.

- Financial institutions introduce new mechanisms for the protection of payment instruments used by consumers. No obtante, esto no significa ni mucho menos que la inversión en seguridad sea óptima, que se vayam a erradicar los fraudes en medios de pago o que los consumidores tengan los conocimientos necesarios para efectivamente aprovechar estos nuevos mecanismos que mejoran su protección.Nevertheless, this does not mean the investment in security is optimal, that fraud in means of payment are going to be eradicated or that consumers have the necessary skills to effectively use these new mechanisms to improve their protection.

LITHUANIA SEMINAR

- Organised by LNCF, National Federation of Lithuanian Consumers
- Vilnius, 16 December 2008
- Ministry of Justice of the Rpublic of Lithuania HQ

National Federation of Lithuanian Consumers (LNVF): LNVF was founded in 2000, its main office is in Vilnius. Its main objetives are the protection of the rights, social and economical interests of the consumers; to train consumers and companies about issues related to the consumption policies and contribute to the development of the security of Lithuanian as well as European consumers. LNVF offers advice to consumers in its offices, by e-mail and telephone informing them about legislation related to any conflict arising between services and goods providers, as well as mediating in consumption conflicts.

PROGRAMME:

10.00 OPENING: Raimundas Jurka, Minister of Justice of the Republic of Lithuania

10:15 INTRODUCTION TO THE STUDY ON FRAUDS IN MEANS OF PAYMENT IN LITHUANIA:
Zilvinas Jancoras, Expert LNCF

10.30 OVERVIEW OF THE FRAUD IN MEANS OF PAYMENT BY THE NATIONAL BANK OF LITHUANIA
Algimantas Sodeika, Director of the Currency Examination Division (Cash Department of the National Bank of Lithuania)
Liutauras Zygas, Director of Jurisprudence of the National Bank of Lithuania

11.10 ACADEMICAL PROPOSAL OF THE VERIFICATION OF MEANS OF PAYMENT
Raimondas Vasiliauskas, Public Security Faculty of the Mykolas Riomeris University in Kaunas

11:30 THE FIGHT AGAINST FRAUD IN MEANS OF PAYMENT IN THE FRAMEWORK OF NATIONAL DEFENSE
Teniente Coronel Saulius Japertas, Director of the Information Systems Service and Communications National Defense Service of the Republic of Lithuania

12:10 PROPOSALS OF THE REGULATATIVE ADMINISTRATION ON THE ISSUE OF PREVENTION OF FRAUDS IN CASHLESS MEANS OF PAYMENT
Rytis Rainys, Director of the Information Security Divistion in the Regulative Agency of Communications of the Republic of Lithuania

13:00 FIGHT AND COOPERATION OF THE POLICE WITH THE STAKEHOLDERS FOR THE PREVENTION OF THE FRAUD IN MEANS OF PAYMENT
Vytautas Gailiusas, Department of Criminal Police, National Lithuanian Police
Aurelijus Banys, Director of the Department of Investigation of Economic Crimes of the Police HQ in Kaunas

Statistical information LITHUANIA

- Increased profit-e-market: since 2003 has increased from 6 to 11.5%.
- More than half of respondents had tried to use smart cards from other people and about 80% had no difficulty in this.
- Over 60% of respondents think that the protection of electronic means of payment is uncertain and poor, about 70% approved the installation PIN code scanners in all storess.

NEW MECHANISMS FOR TESTING MEANS OF PAYMENT

Academic institutions as precursors of new methods for combating fraud in the means of payment

The Faculty of Public Security University in Kaunas Mykolas Riomeris has considerable experience in the fight against fraud in various areas. This institution has developed a new method to verify the authenticity of documents (which, for example, may be used for means of payment) using a system known as "specific radiating waves" (in Lithuanian, Kriminalistinės holografinės interferencijos methods).

This new method is based on the graphic recording of the volume of objects, so as to protect documents (which, as we said, can be applied to means of payment) against attempts of fraud.

The advantages of deploying this new method are, among many others, ensuring the preservation of the status of the original object. In addition, this method allows to obtain copies of the object or impressions that relate to its full three-dimensional features in a way that maintains the security and permanence of the individual traits of each of these methods and holograms that could be used as evidence in court .

The researchers were funded by the "Twins Project" (Project Twins) although results have not been yet officially published. Representatives of this University expect that this method will help the manufacturing process of Euro notes and coins and in the investigation against the counterfeiting of other systems of payment other than cash.

COMBATING FRAUD IN MEANS OF PAYMENT UNDER THE NATIONAL DEFENSE

Experiences of the police in cooperation with other actors

Currently, the Police is involved in various interdepartmental working groups, which together with the representatives of different institutions (banks, Ministry of National Defense, Ministry of Foreign Affairs, Ministry of Transport and Communications, National Bank, Ministry of Internal Security Department State, Ministry of Finance and departments, etc.) made proposals for the government to strengthen information security..

There are a number of actors in which the movement of electronic payment cards concerns: police, prosecutors, courts, central banks and commercial companies that produce and authorize electronic cards, which perform functions subject to control and education and international organizations.

There was a big case of fraud in means of payment other

than cash committed by a criminal group in Sri Lanka and individuals Lithuanians. This scam was that criminals were using fake electronic cards to draw money from ATMs.

However, most of the crimes are carried out by the use of electronic cards that have been truly stolen while he was paying for something or trying to get money.

The police believes that there is not enough explicit rules about who should be compensated in case of fraud (bank, shop, etc).

Currently, such a working group chaired by the Director of Defense Policy and Planning Department of the Ministry of National Defense, focuses on creating a legal basis in cybersecurity, developing a national system of coordination, the prevention of threats, the creation of response systems, the pursuit of infringements, the implementation of safety standards in implementation of security technologies, international cooperation and the formation of the national culture of cyber security.

INITIATIVES OF PUBLIC ADMINISTRATION IN THE FIELD OF PREVENTION OF FRAUD IN THE MEANS OF PAYMENT

The Regulatory Authority for Communications is the main institution that defends the rights of consumers by ensuring competition in the markets of electronic links, shipping and delivery of quality services.

The mission of this institution is to ensure the variety of affordable electronic communications, technologically progressive, of high quality and security, and postal services (products) to every citizen of Lithuania as a prerequisite for the development of information society.

In addition, the Communications Regulatory Authority is an institution that participates in the process of dispute resolution between consumers and service providers.

CONCLUSIONS

- Unlike other countries, Lithuania is not ready to protect itself from potential attacks, since there is no international system of protection and each country is responsible to protect their economic and administrative machinery.
- As in other EU countries, which generally is considered that so far there has been a lack of clear rules on the assumption of liability in case of fraud (financial institution, issuer of the means of payment, or user).
- The promotion of R & D activities related to the technical security means of payment are vital for combating economic crimes associated with these instruments.

BULGARY SEMINAR

- Organised by BNAP, Bulgarian National Consumer Association
- Sofia, 28 January 2009
- Sofia, 28 January 2009

The National Consumer Association in Bulgary is a NGO founded in 1998 which has as its main objective the protection of the rights of consumers in Bulgaria. This is why BNAP provides information so the consumers can choose better among the different products, offers a juridic advisory service to do judicial and out-of-court claims, and is present in the legislative processes representing consumers.

PROGRAMME:

09:00 OPENING OF THE SYMPOSIUM BY DANIELA IVANOVA, PRESIDENT OF THE NATIONAL CONSUMER ASSOCIATION IN BULGARY
COMMUNICATION BY THE EUROPEAN COMMISSAR FOR CONSUMERS, MEGLENA KUNEVA

09:55 VULNERABILITIES OF MAGNETIC CARDS AND FORENSICAL ANALYSIS
Catalin Grigoras, Forensical Expert from Romania.

10:15 LEGISLATION FOR THE PROTECTION OF THE USER AGAINST COMPUTER FRAUDS
Doctor Georgi Dimitrow, Law and Internet Foundation.

10:35 INTERNET THREATS AND CHALLENGES IN ISRAEL FOR THE PREVENTION OF THE FRAUDS
Avi Linden, Fraud Protection Expert, Israel

11:30 PRESENTATION OF THE STUDY OF FRAUD IN MEANS OF PAYMENT IN BULSGARY
Bogomil Nikolov, Director of the National Consumer Association in Bulgary

11:50 POINT OF VIEW OF THE FINANCIAL ENTITIES IN BULGARY
Eleonora Hristoforova, Lawyer of the National Bank Association in Bulgaria.

12:05 THE FIGHT AGAINS FRAUD BY THE PUBLIC ADMINISTRATION
Yavor Koev, Director of the Section of Computer Crimes, Sudbirection of Fight against Organised Crime of the Ministry of Internal Affairs

ATTENDANTS: Over 60 people in total, with representatives of the Police, representatives of diverse Ministeries, banking sector (Allianz Bank, Piraeus Bank, Corpbanc Bank, Municipal Bank, PostBank, Fibanc), companies (Mastercard) and representatives of consumption institutions.

DIFUSSION: There were media covering the event, such as the TV channel TVEuropa, who interviewed the director of BNAP. In addition of thi, there was issued a press review about the event published by the main Internet newspapers, like News.bg, Segabg.com, Ekipnews.com, Focus-news.net, Dnevnik.bg, Darikfinance.bg y Hicomm.bg.

Statistical information BULGARY

- Insecurity, problems and user dissatisfaction Bulgarian Means of Payment.
- 60% of Bulgarian consumers have had problems with payment cards.
- Up to 22% of consumers do not feel completely sure that the payments are not made in cash.
- Up to 29% of consumers found that the cost of the payments are not made in cash is high, while 63% think it's normal.

STUDY ON FRAUD IN THE MEANS OF PAYMENT IN BULGARIA

There are provisions for the protection of users of means of payment fraud in the various legislation in Bulgarian:

- Constitution of Bulgaria.
- Law of Consumer Protection.
- Provision Act-distance services.
- Law on Electronic Commerce.
- Law on money transfers, electronic payment instruments and payment systems.

In the extrajudicial resolution of discrepancies between user and company, it is the Conciliation Commission in Conflict Payments the organism encharged of mediating between both parties.

The Commission for Conciliation Conflict Payments is a tool for resolving conflicts in Bulgaria out of court. Is an independent body, consisting of two representatives from the Association of Commercial Banks and two representatives of the Commission on Consumer Protection. The president is a representative of the Bulgarian National Bank, ie he or she is not committed to either side of the conflict.

The Conciliation Commission is created under the Law on the transfer of money, media and electronic payment systems and has authority to act under the following circumstances:

- Conflicts over money transfers between banks and other licensed operators on the one hand, and its other customers;
- Conflicts on issues of electronic payment instruments (especially cards) between banks and other licensed operators on the one hand, and its customer on the other.

We already find in Bulgarian courts fraud matters in means of payment, even though there are very few cases. In this regard, we find the sentence number 252/14.05.2007 ruling of the Court of Final Appeal on identity theft and forgery of a credit card and economic damage by 10,964.90 lev (about 5595 euros). The accused was charged with 5 years and 6 months of imprisonment.

LEGISLATION FOR THE PROTECTION OF FRAUD IN COMPUTER USERS

- Criminal protection: This type of protection envisaged in the Criminal Code of Bulgaria, under Chapter V, Section IV.
- Civil Protection: The liability of Internet providers is reflected in the Bulgarian Law on Electronic Commerce.
- Administrative Protection: The work of the Committee on Consumer Protection has focused on this aspect. La pena por enviar estafas a personas o compañías, bajo la Ley del Comercio Electrónico Búlgaro, varía entre los 500 levas y los 2000 (250 – 1000 euros). The penalty for sending frauds to people or companies, under the Bulgarian Law on Electronic Commerce, varies between 500 cam and 2000 (250 - 1000 euros).

In the Law on Protection Commission, are included penalties for unfair competition case relating particularly to the cases of commercial fraud.

VULNERABILITIES OF THE MAGNETIC CARDS AND FORENSIC ANALYSIS

Vulnerabilities in magnetic cards can be analyzed from a forensic point of view, as stated Catalin Grigore, Romania Forensic Expert.

The magnetic cards are governed by rule ISO 7810, which is a standard that defines the physical characteristics of identification cards or identification.

Formato	Dimensión
ID-1	85.60 × 53.98 mm
ID-2	105 × 74 mm
ID-3	125 × 88 mm
ID-000	25 × 15 mm

The standard defines four different sizes of cards: ID-1, ID-2, ID-3 and ID-000.

Falsification of the magnetic stripe and fraudulent use.

The main methods of falsification of magnetic cards and subsequent fraudulent use consist mainly of reading the contents of the original banda magnetic recording, capturing the PIN code entered on the keyboard and back copy of the contents of the card involved in a new card (which can be either a stolen card or a blank card).

In practice, there are cases of data theft at the time of reading the card (skimming) for reading devices (ATM, point of sale terminal). To visually check the abovementioned, we see only a card reader, if there are two, it could be that there is an apparatus with which they intend to execute subtraction techniques for reading data.

Some of the technical solutions against counterfeiting of credit cards by this method are as smart cards (which provide additional verification mechanisms) or contactless card.

TYPES OF INTERNET FRAUD AND CHALLENGES AS TO ITS PREVENTION

THE VISION OF THE PRIVATE ENTERPRISE IN EUROPE AND ISRAEL

The department responsible for the risk in various financial institutions face many challenges: a dynamic regulatory standards and increasingly rigorous, a highly competitive business, widespread adoption of electronic banking and electronic payments, complex data infrastructure and a continuous development and immigration of fraud.

As a result, those responsible need solutions that provide them with leadership skills in these areas.

What are the frauds that most concern financial institutions in Israel?

1. Fraud at cash points / debit cards

One of the challenges is discovering more fraud in real time and to protect consumers through products and marketing channels: this action must be based on cooperation between the various financial institutions entities, and with input from consumers.

Some incidents related to the large volume of some compromising information in cardholders are worrying consumers, legislators and the card industry. Under the pressure of taking action against it, card issuers are being forced to take various measures, which must be added to the cost of replacing large quantities of cards.

Some fraud attempts continue influencing transnational strategies to combat fraud by institutions, resulting in a greater impact to cardholders traveling abroad.

Debit cards are increasingly used for online purchases and certain non-face card fraud continue to be the type of fraud which is increasing at a faster rate in recent years. These factors represent a significant challenge for the institutions since they must follow all developments in terms of new cases of fraud, these evolving with increasing speed.

2. Employee fraud.

Financial institutions are very concerned about fraud caused with the consent, cooperation or bad faith of its employees. These may consider autocontratación, embezzlement, data theft, violations of company policy and other similar issues, they represent a significant challenge for financial institutions.A recent survey on the financial services industry reveals that 65 percent of respondents believe tueres has been an increase in the risk of fraud by employees, including over 60 percent who believe that their abilities to detect fraud by employees is less than what would be acceptable.

3. The prevention of fraud to businesses - business solutions.

Fraud prevention is an ongoing and evolutionary activity, because the criminals are changing tactics and developping new strategies. Detection systems which are compartmentalized and disjointed are inefficient, costly and discover less frauds than multiple solutions boosted by a single platform. To avoid losses, regulatory interventions and damage to brands, companies need to broad skills to prevent corporate fraud that offer a common platform to reduce false positive rates and automates manual processes.

4. Isolated bank fraud - protection through the product and through the channel.

The rapid growth in the number of access channels and complexity in the banking industry has created new business opportunities for financial services companies, but has also created new challenges to the fraud. The scammers are addressed systematically to a variety of broad access channels, such as call center, online sites, and mobile banking systems, interactive voice response. Due to the anonymous nature of these channels and the growing range of services available through these remote channels, financial institutions face unique challenges and should not only avoid monetary losses, but to send the erosion of confidence of the end user in payment systems.

PROPOSALS FOR THE FIGHT AGAINST FRAUD OF THE FINANCIAL INSTITUTIONS IN BULGARIA

The Association of Banks in Bulgaria has implemented a number of legislative proposals in this area, actively intervening in the legislative processes in Bulgaria as well as other actions aimed at improving coordination between banks and the Bulgarian authorities.

The Association of Banks in Bulgaria combating financial fraud through its Security Committee, made proposals which are generally considered and accepted by financial institutions Members.

THE GOVERNMENT OF THE FIGHT AGAINST FRAUD

- Computer Crimes Section of works for him in the persecution and elimination of bank robbery by criminal groups of Bulgarian and international.
- There is a common project of the Ministry and Microsoft, the Web Cybercrime.bg, which addresses some of the issues addressed in the Symposium. This site was designed by students of the School of Electronics Vocacionesl John Atanasov, along with the Corps for the Fight against Organized Crime, and with financial support from the Veterans Association of Police.

This website offers tips for users in terms of protecting data against various scams such as phishing.

CONCLUSIONS

- The fraud-in means of payment other than cash is a common problem for consumers, banks and institutions, and increasingly important in Bulgaria, despite the fact that at present it can be seen that the levels of heading are rather low.
- Financial institutions and businesses still have much to improve in relation to protection of their clients against the means of payment fraud, as evidenced by the relatively common cases of compromised information that is made available to criminal gangs specializing in this type of economic crimes.
- The coordination between the banks to ensure safe access for users to e-banking is of crucial importance.
- The fight against fraud in payment means it is vital not only in relation to ensuring the rights of consumers, citizens in general and the State of Law. This type of economic crimes are commonly associated with cases of black money laundering, drug and weapon dealing, terrorism, etc.., so when we are struggling to fight against them we are fighting against many other types of criminal activities.

ITALY SEMINAR (I) ADICONSUM

- Organised by ADICONSUM, Association for the Consumer and Nature Defense
- Roma, 30 January 2009
- Cavour Conference Centre

ADICONSUM: The Association for the Defense for Consumers and Nature is a consumer association with over 122.000 associates, constituted in 1987 by the CISL (Italian Confederation of Trade Unions). ADICONSUM defends the interests of consumers independently from companies, political parties, Government and trade uniones. It is present in all the italian regions, with 283 information centres and advisory services for consumers in the main cities. ADICONSUM has 35 full-time workers, 105 part-time workers and hundreds of volunteers.

PROGRAMME:

OPENING: Paolo Landi, General Secretary of ADICONSUM

THE POINT OF VIEW OF INSTITUTION AND LAW ENFORCEMENT AUTHORITIES

Antonio D'Onofrio, Director of the Department of cyber crime of the Special Unit of the financial Police for the Telematic Fraud (G.A.T.);

Giovanni Pollastrini, Director of the Area of Card Payment and Credit for Consumotion, UCAMP (Antifraud of Means of Payment Central Office of the Ministry for economy and Finance)

THE POINT OF VIEW OF INDUSTRY AND PRIVATE ENTITIES

Alessandro Zollo, Director of sales and means of payment of the Italian Bank Association (ABI);
Enrico Lodi, Director of the Office of Credit Service of CRIF (Credit Information Service);
Vincenzo Leggiero, Director of marketing of Consum.it - Monte dei Paschi di Siena Group;
Raffaele Panico, Fraud Management, Poste Italiane;
Antonio Caricato, Security and Business Director of the Central Institute of Popular Banks in Italy

THE POINT OF VIEW OF THE ACADEMICS

Fabio Picciolini, Expert in Banking and Finance
Mara Mignone, Investigator of the Centre of Investigarion about Security and Crim(RISSC)

Statistical information ITALY

■ Italy is a country with relatively low figures for the use of the various services available to Internet users.

■ 20% of Internet users use it to search for Italian travel and accommodation.

■ 17% of Internet users use it to read Italian newspapers and news.

■ Only 7% of Internet Italians users use it to look for work or purchase goods or services. This figure is worrying for the European Commission, because it runs in an opposite direction to the increasingtrade and labor integration among member countries.

EXPERIENCE AND ACTIVITIES OF THE ASSOCIATION OF ITALIAN CONSUMERS IN THE ERADICATION OF ECONOMIC CRIMES ON PAYMENT SYSTEMS OTHER THAN CASH

The means of payment frauds have become part of the lives of many Italians. It has been discovered over 22,000 cases of fraud and what is more worrying, this type of cases have doubled in recent years..

There is a wide variety of different types of fraud, from the relatively simple theft of credit cards to more complex scams like identity theft.

ADICONSUM akes time to work on consumer protection to the means of payment fraud;it particularly has been active in the consultative process of variouslegislative texts related to this subject:

- Consolidated text adopted by the Standing Committee (Bill No. 414 and 507) Provision for the fight against identity theft and fraud prevention in the field of consumer credit, deferred payments of the insurance industry

- Arguments form ADICONSUM to the Laws 414 and 507 on Fraud Prevention in Consumer Credit and deferred payments, referred to the Finance Committee of the Senate of the Italian Republic.

THE VISION OF INSTITUTIONS AND SECURITY FORCES

Banking and postal sector had conducted extensive efforts undertaken by these agencies to try to reduce the economic damage that users face when they are victims of such fraud.These institutions believe that more resources should be devoted to police investigations in order to reduce the consequences of such crimes.

There is expressed willingness of the public sector in the protection of users as well as monitoring and controling of such crimes. In this regard, some of the best measures of the government accepted by all actors involved in this problem are the creation of a database that will collect credit card information and the resumption of parlamentary debate on an effective system to combat fraud on financial consumption. .

INDUSTRY INITIATIVES AND PRIVATE ORGANIZATIONS IN THE PREVENTION OF FRAUD IN THE MEANS OF PAYMENT

The Italian Banking Association reached an agreement with the Consortium for Bancomat which will replace all of the POS (Point of Sale Terminal) for a further verification with EMV-Chip system, much safer, by making available to the banking system Presidio Sicurezza Moneta. "Since 2007 the fraud phenomenon trend has reversed, thanks to these initiative decreasing in a 30% the following year.

However, fraud in the country composes a small proportion in relation with all cases of fraud, so the Bancoma Consortium envisaged under the Strategic Program, the creation of a "Fraud Competence Center, "which will have a positive influence in the prevention of credit card fraud around the world.

The creation of SIPAF, an informatic file that was discussed at the second seminar in Rome, is an important initiative

in the prevention of fraud in payment means in Italy.

Two of the speakers, a criminologist and an officer of the Guardia di Finanza (financial police of Italy) made contributions of great interest. In particular, the representative of the GAT-Fraud Unit for Telematic Financial Police explained that there are many other ways to make users not to be aware, although it is also possible to implement a large number of measures that have a real effect as to minimize the damage caused by fraud.

CRIF is an Italian company that performs services for financial traders, businesses and citizens both domestically and internationally, so they can have accurate information and findings.

In Italy, consumers are more than 10,000 subscribers to the service of personal data protection against credit fraud offered by CRIF (IDENTIKIT), which uses the big amount of information and experience in this field of CRIF. This system provides an alert when a change occurs regarding the credit standing of the client, caused by dany attempt of credit fraud by illegal use of customer data.

THE VISION OF ACADEMIC: Consumer confidence cracked

Ms Mara Mignone, criminologist representative of RISSC (Center for Research and Crime and Security Survey) conducted a technical presentation by defining from a criminologist's point of view the characteristics of the non-cash payments, electronic money and the fraud they may suffer as a criminal phenomenon.

Mignone said that some data obtained under the Project Nessun conducted by CRIF RISSC with CCP and Italy in 2007, including:

- About 88% of respondents were using the ATM, although the percentage was reduced to 65% for those who use credit cards.
- Most respondents have a frequency of use of cash points "several times a week or several times a month." The credit card is primarily used "occasionally".
- The owner of the credit card or cash point user a "significant uncertainty" in the use of the credit card as an alternative to cash. This uncertainty conditions, however, in a diverse way the habits and methods of payment and use of electronic payment.
- Cash point users don´t not use credit cards because they do not feel safe. Only the use of it abroad is more limited. The holder of a credit card, uses it abroad only if he feels safe enough.
- There is a widespread fear of suffering fraud and identity theft with credit cards. In fact, 90% of those interviewed stated that they "fear of being victims of fraud in means of payment"
- The 92.11% of ATM users and 91.91% of credit card holders are afraid of becoming victims of fraud in the means of payment.

These fears, in fact, can be considered justified and that 38% of respondents had any experience as a direct or indirect victim in the past year.

However, it is true that most citizens (61%) were attentive to the safety of their personal information, paying attention when giving it even at most frequent situations. The most common are those involving the least effort possible, and are often in line with data transmitted by the media generator: the signature of the card (65%), a generic warning to pay (61%), destruction of the card, a time lapse (58%). The rate starts to decrease significantly when discussing activation of SMS alerts (30%), verification of receipt of the credit card during the period of time (18%) and activation of various anti-fraud services to Internet purchases, such as Verified by Visa, MastercardSecureCode-(18%).

The above survey was conducted with more than 400 people in the italian towns of Padua, Milan, Rome and Naples.

There is therefore a problem of awareness, care and education of citizens regarding to security, there is nevertheless a problem of excessive alarmism and not always an accurate representation of the real situation.

For all the above-mentioned questions, RISCC in collaboration with UCAMP has embarked on the national (Central Bureau Fraud Means of Payment in the Ministry of Economy and Finance) Project ALIAS-Strengthening public-private cooperation against theft fraud and identity cards. (http://www.rissc.it/alias) The main problem that this project tries to address is the evolution and rapid spread of fraud schemes, an emerging issue across Europe plus Italy.

CONCLUSIONS

- It is necessary to start a real debate in Italy on the fight against such crimes, which are particularly insidious because it is relatively easy to commit and very difficult to detect (at least in terms of time is concerned).
- It is a very important aspect the need to improve legislation and increase international cooperation, considering that this type of crime has no boundaries and no separation between countries.
- It is very necessary to carry out the fact that users should have at its disposal a number of mechanisms in terms of its easy application for protection.
- The problem of fraud in means of payment should be continuously monitored and reminded to users and consumers through advertising campaigns in the media and in legislative proposals for new developments.

ITALY SEMINAR (II) MDC

- Organised by MDC, Movement for the Defense of the Citizen
- Rome, 13 February 2009
- University Rome III

Movimento Difesa del Cittadino (MDC): The Movement for the Defense of the Citizen was founded in Rome in the year 1987 with the objective of promoting the defense of the rights of the citizens, informing and providing them with self-defense tools, helping and advising by experts. MDC has a Juridic Advisory Office and a Press office, amoung other more specific departments.

PROGRAMME:

14.00 OPENING AND PRESENTATION OF THE PROJECT:
Antonio Longo, President Movimiento Difesa dei Cittadino

PRESENTATION OF THE RESULTS OF THE STUDY OF THE SITUATION OF FRAUD IN MEANS OF PAYMENT IN ITALY

ELECTRONIC MEANS OF PAYMENT: TUTELATION OR FREEDOM OF THE CONSUMER?
Federico Regaldo, MDC Lawyer and Responsible for the Study

EXPERIENCE IN THE ISSUE OF FRAUD IN MEANS OF PAYMENT WITHIN THE ACTIVITIES OF CONSUMER ASSOCIATIONS
Mattia Cappello, MDC Lawyer

THE POINT OF VIEW OF INSTITUTIONS AND LAW ENFORCEMENT AUTHORITIES
Antonio D'Onofrio, Director of the Cybercrime department of the Special Unit of the Financial Police for the Telematic Fraud (G.A.T.);
Giovanni Pollastrini, Director of the Area of Card Payment and Credit for Consumption UCAMP (Central Antifraud Office if Means of Payment of the Ministry of Finance and Economy)

THE POINT OF VIEW OF THE INDUSTRY AND PRIVATE ASSOCIATIONS
Alessandro Zollo, Director of sales and means of payment of the Italian Baking Association (ABI)
Raffaele Panico, Representative of the National Post Service in Italy (Poste Italiane)
Luigi Altavilla, Banco Unicredit
Antonio Galiano, Banco ICCREA

THE POINT OF VIEW OF THE ACADEMY: THE PROTECTION OF THE SAVERS IN FINANCIAL SERVICES
Ettore Battelli, Investigator University Roma III.
Liliana Rossi Carleo, Coordinator of Master "Globalisation of the Markets and Protection for Consumers", University Roma III

Statistical information ITALY

■ The number of italian families that have Internet access has grown in recent years. It has risen from 40% in 2006 to 42% in 2008 (source: Eurostat) However, despite the relatively small percentage of Internet connection (in Sweden, for the year 2008, the percentage of families connected is exactly twice) we see that it progresses very slowly, contrary to what one would expect, ie rapid increases from 2006 levels, as that observed in Spain, Portugal, Estonia and Latvia).

PRESENTATION OF RESULTS OF STUDY ON THE STATUS OF FRAUD IN THE MEANS OF PAYMENT IN ITALY

The italian legislator drafted the Law 206 of 2005 (the "Consumer Code), establishing that the contracts for online and other forms of contracts of non-attendance" the card issuer must reimburse the consumer all payments for which consumers provide evidence that there is an excess in the price, compared with the previously agreed price or fraudulent use of cards by the subsidiaries of commercial establishments or others "

The same principle has also applications in on-line financial services for consumers, in accordance with section 67 of the Consumer Code, as introduced under section 9 of Act No. 221 of October 23, 2007. There are some gaps or problems in the interpretation of these rules, but, under this Act, the protection of the user from this type of payment (card) has been strengthened considerably.

Banking institutions and consumer associations have witnessed in recent times that the online scam in electronic payment is a major social issue

THE VISION OF INDUSTRY AND PRIVATE ENTITIES

Views on the relevance and future of means of payment in Italy

The Unicredit bank, one of the leading providers of On-Line Banking, expressed his concern about this phenomenon and explained its commitment to eradicate such crimes, since 40% of their clients operations are through Electronic Banking .

Criminal prosecution of perpetrators of crimes on the net , while theoretically possible, in practice does not represent a viable solution. As an example, one can cite a legal process started in Russia against the perpetrators of this fraud that in the end had no consequences for the victims of it.

Therefore, Unicredit also stressed the need to focus on the aspect of prevention to eliminate fraud in means of payment other than cash, and to clarify that in order not to blow the trust that customers have in these remote banking mechanisms of recruitment , Unicredit was prepared to take responsibility and repay the amount stolen to the victims of fraud in most cases.

ABI, the association that includes commercial banks operating in Italy, stressed that the assumption of responsibility is a fact already on the market for credit card payments, while the owners of new cards (those that come with both magnetic stripe and chip) should be exempted from liability in cases where it is delivered to the shop and attached to the payment that is made not by the chip on the card but by the magnetic stripe.

ABI also highlighted as major reasons for the predominance of the use of cash in Italy the following issues:

- Cultural barriers to the use of electronic money.
- Short-range of POS -Point of Sale- between small businesses (only 16.5% of pequelos merchants offer card payment).
- Lack of alternative to cash for small payments.
- High-fragmentation of the economic fabric.

It can be highlighted as positive features for consumers in the use of cash payments to the total spread of its use, the increased speed of transactions, the anonymity, the absence of costs to users and a greater sense of control of expenditure. On the other hand, negative aspects include the use of cash, as the cost to the overall system (production costs of coins and banknotes, security of) the impossibility of making purchases online, the physical limit their spending power- it is limited to the amount of which is available at that time- and the possibility of theft and fraud associated with its use.

It also was explained the agreement reached with the consortium ABI BANCOMAT (ATM network in Italy) in collaboration with the Ministry of Economy and Finance and UCAMP (Central Office for Combating Fraud Means of Payment). This agreement results in the creation of SIPAF, computer file containing information useful for preventing credit card fraud and was established on December 1, 2008. Esta iniciativa, en la cual participan 700 entidades financieras y This initiative, involved 700 financial institutions.

Some of these issues were also confirmed by the financial institution ICCREA: the means of payment fraud enables the electronic means of payment among consumers and therefore hinders the process of reducing costs associated with less use of notes and coins. Therefore, banks have real and substantial incentives to combat this problem, which is based not only on the need to repay the amount stolen to the consumer who has been a victim of fraud. Analyzing the most developed service markets of the means of payment (eg United Kingdom) ICCREA anticipates that for the Italian market, there will be a reduction of fraud using skimming, but that this reduction will contrast with the less strong increase in non-presential fraud and identity theft (in United Kingdom, attendance fraud involved a total of 52%, compared with 29% in Italy)

The public postal service in Italy, Poste Italiane SpA, is today a leading provider of global e-banking services, with more than 4 and a half million customers and is equipped with several special units dedicated to prevent fraud in the means of payment.

According to Poste Italiane, the phenomenon is quite serious: for example, the Internet provides anti-phishing kits for € 200-300 for the protection of users from such attacks. Such crimes are not punishable by imprisonment (if previously other crimes haven´t been committed) and phishing attacks is increasing dramatically from 67 in 2007 to 6700 in 2008.

In addition to suggesting the use of the special care service Internet banking (eg, check that the website is a protected domain, identified by the "https" addresses the bar-and that, moreover, the symbol a lock on the website. It is also important to keep your computer protected with a antivitus and to not be requested more than 4 characters for identification, etc.). Poste Italiane announced the introduction of a new mechanism, a kind of personal card reader necessary for trasnfering money online. This will establish an additional security measure independent of the Internet, which is expected to increase.

THE VISION OF CONSUMER ASSOCIATIONS

Main barriers to the enforcement of consumer rights:

- Lack of information for consumers about their rights when, having been victims of one of these scams, they go to offices of the associations. In this sense, Movimento Difesa dei cittadino, the organizer of the seminar, has posted on its website most of the workshop and interviews with participants for it to be watched on-line.
- The mediation efforts, partnerships between banks and other institutions are excluded from the electronic payment. This is a nuisance for most victims of fraud, which is particularly unwarranted given that other technology sectors (eg, discrepancies in terms of programs that redirect to premium rate lines from the user's PC) enterprises have agreed to conduct negotiations directly with the consumer associations.

CONCLUSIONS

- It is considered that responsibility be should assumed, at least in certain cases of fraud, not by victims but by financial institutions or card issuers, following the path already set by the Directive (EEC) 85/374 on responsibility for damage caused by defective products

- The lack of information for users of means of payment other than cash is still notable in their rights as consumers, and channels that can be used to restore an unjust situation or conflict with a primary means of payment or entity financial..

- It is necessary to increase international cooperation among judicial authorities of different countries, as the prosecution of perpetrators of crimes on the net in most cases presents great practical difficulties. En muchos casos de fraude electrónico al final no se da ninguna solución práctica para las víctimas del mismo. In many cases of fraud in the end there is no practical solution for the victims of it.

ROMANIA SEMINAR

- Organised by ANPCPPSR, National Association for the Protection of the Consumer and the Promotion of Strategies in Romania
- Bucharest, 23 March 2009
- Ion Heliade Radulescu Room of the Library of the Romanian Academy (Calea Victoriei, 125, Sector 1, Bucharest)

The National Association for the Protection of the Consumer and the Promotion of Strategies in Romania (ANPCPPS Romania): Founded in Bucharest in 2003, ANPCPPSR is a NGO which is aimed at protecting the legitime rights and interests of romanian consumers, informing them about their rights and integrating them in the social life. One of its activities is te creation of quality standards.

INTERVENTIONS BY:

Sorin Mierlea,
President of the National Association for the Protection of the Consumer and the Promotion of Strategies in Romania

Adrian Trandafir,
General Inspector of the Romanian Police – General Direction for the Fight against Organised Crime

Răzvan Resmeriță,
Director of the European Consumer Centre (ECC-Net) in Romania

Alexandru Molodoi,
Oficial Technician Director, Gecad-Net

Doctora Virgina Campeanu,
Director of the Institute of World Economy (IEM) "Costin Murgescu"

Juanjo Machado,
Responsible of International Relationships of the Association of Users of Banks, Savings Banks and Insurances (ADICAE)

Juan Manuel Viver,
Responsible of International Projects of the Association of Users of Banks, Savings Banks and Insurances (ADICAE)

Mugur Amariei,
Expert of the National Association for the Protection of the Consumer and the Promotion of Strategies in Romania

Statistical information ROMANIA

- There were 12 million Internet users in March 2008, with a 53.9% penetration, according to ITU (International Telecommunication Union). There has been a growth in use from 2000 to 2008 of 1400%.
- There were 1,769,300 connections, broadband Internet in September 2007 (according to ITU), which suppose a penetration of 7.9%. As for Internet users in August they were 5,062,500 in 2007, 23.9% of the population.
- According to Eurostat, the EU countries with fewer Internet shoppers are Bulgaria and Romania (both 3%) This figure contrasts sharply with the seven EU countries where there are more Internet purchases, in which the half of its citizens made a purchase on the Internet in 2008. These are Denmark, United Kingdom, Holland, Germany, Sweden and Finland.
- In terms of percentage of online payments for e-commerce market it was 15% ol 20% in 2007. Growth is important, since it is estimated to be a 25%by 2008.

LEGISLATION FOR THE PROTECTION OF THE USERS OF MEANS OF PAYMENT IN ROMANIA

Experience and views of the National Police Force of Romania.

Cyber Crimes Directorate within the Department against Organized Crime, is the romanian department of National Police Corps to combat fraud in the means of payment other than cash in Romania.

As for the skills developed by the Cyber Crimes Directive of the National Police of Romania, it should be noted, first, preventing and fighting cyber crimes (auction fraud, illegal access to computer systems) and crimes committed with instruments of electronic payment. International and institutional cooperation at the international level, cooperation in general with the public and private sector are proving to be very necessary for the fight against such crimes.

It is quite common that when we talk about the electronic payment is usually associated only with credit cards. In accordance with the romanian laws (Law on Electronic Commerce, no. 365/2002) an electronic payment instrument is a system that allows the user to do the following:

- Transfer of funds other than those carried out by financial institutions.
- Removal of money through cash points, in addition to available cash or instruments of electronic money

Also, the Law No 365/2002 (Article 1, points 11 and 12) provides two types of electronic payment instruments:

- Payment instruments of Remote Access: Allows users to access their funds, which are available in a financial institution and authorize a payment using a personal identification code or similar identification system. Example: On-Line Banking
- Electronic money instrument: It is a reloadable payment instrument different from the payment instruments of remote access, in which value units are stored electronically, enabling its owner to perform any of the transactions described in the Act (transfer funds, obtain cash)

PENALTIES

Counterfeiting of electronic payment is punished by 3 to 12 years and the abolition of certain rights.

The manufacture or possession of equipment, including hardware and software to be used in the counterfeiting of electronic payment, is punishable by imprisonment from 6 months to 5 years.

Forgery in statements to the issuance or use of electronic payment is sentenced with imprisonment from 3 months to 12 years.

The use of an electronic payment without the consent of its owner, including identifying the passwords that allow their use is punished with imprisonment from 3 months to 2 years.

Acceptance of financial transactions, even knowing that those who commit it are falsifying or using electronic means of payment without the consent of its owner, is punishable with imprisonment from 1 to 12 years.

Romanian National Police has conducted police actions in cases of fraud involving not only interconnections across Europe (Romania to Italy, Spain, Ireland, United Kingdom, Holland, Sweden, Germany and Cyprus), but also throughout the world (Europe to U.S. , Brazil, Australia, Thailand, China, Tunisia).

For the development of education and information for consumers about the fraud in means of payment aspects, the Romanian consumer association ANPCPPS participates in a working group in this area, to maintain a proactive dialogue between the concerned parties (authorities, NGOs, banks, consumers, etc.) and establishing a national strategy in this regard, with the aim of reducing the number of cases of fraud in the means of payment.

CONCLUSIONS

- Tere is a need to provide better consumer education and information, plus practical ways to combat fraud, especially in countries where the means of payment are less widespread.
- Need to have secure web application to set high safety standards in the operations of remote users of means of payment, and increase security of presential payment transactions.
- The creation of groups monitoring the means of payment fraud in each country, with the collaboration of all actors at national level related to the problem associated with the use of payment instruments is essential to strive for the eradication of such Crimes.

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

SLOVAK REPUBLIC SEMINAR

- Organised by ZSS, the Slovak Association of Consumers
- Bratislava, 7 April 2009
- Odborarske namestie, 3 (Intitue of Tourism and National Office for the Protection of Data HQ, etc)

"Združenie slovenských spotrebiteľov (ZSS): The Slovak Association of Consumers was founded in 1990; it is the only association of consumers that operates in the whole territory of Slovakia, with its main office in Bratislava. Its main duties are the advisory service and education of consumers, as well as undertaking legal inicitives in the legislative processes which affect consumers.

PROGRAMME:

THE POINT OF VIEW OF THE CONSUMER ASSOCIATION. THE PROTECTION OF CONSUMERS AGAINST THE FRAUDS IN MEANS OF PAYMENT IN THE REPUBLIC OF SLOVAKIA

THE POINT OF VIEW OF THE INDUSTRY AND PRIVATE COMPANIES

INTERVENCIONES DE:

Miro Túlak,
President of Slovak Association of Consumers

Juan Manuel Viver,
Coordinator of the Project and Responsible of International Projects of ADICAE

Gabriel Tocka,
representative of TESCO supermarkets in the Slovak Republic

Olga Petrovicova,
representative of financial entity UNICREDIT

Roland Katona,
Director of the Section of Bank Cards of CSOB Bank (KBC Group)

Robert Bohunicky,
representative of the Department against Counterfeit and Computer Crimes of the National Police of the Slovak Republic HQl

Statistical information SLOVAK R.

- According to Eurostat, the Slovaks users are increasingly entering more and more frequently on the Internet. The situation changed from about 27% of households with Internet connections in 2006 to a rate of 58% in 2008.
- Slovak-users use the Internet mainly to check newspapers and online news (34%), performing paperwork (30%), recruitment and search for accommodation and transport services (29%) and search for health information (25%)
- The percentage of Slovaks who use electronic banking is 24% .

HISTORY OF MEANS OF PAYMENT IN SLOVAKIA

Development throughout the history of payment cards in Slovakia has been long, with milestones like the first payment card (or system with the same purpose) by the Western Union Telegraph Company. In 1950, Diners Club began to be emmitted, a more sophisticated version, in addition to that emitted in 1951, the Franklin National Bank of New York .Iwe can say that it is in 1958 when Bank of America began to issue cards that operated like the ones we use today

Specifically, Slovakia (formerly Czechoslovakia) in 1968 when the travel agent Čedok began accepting foreign credit cards as payment. The first credit cards are not issued in Czechoslovakia until 1988, the Bank Zivnostenska Banka, and in 1989 the savings bank Česká spořitelna státna.

However, it´s only possible to say that in 1992 Czechoslovakia adopts the most modern mechanisms in terms of credit cards, comparable to other countries with more tradition in these means of payment

THE CONSUMER FRAUD IN THE MEANS OF PAYMENT IN SLOVAKIA

Consumer associations of Slovakia believe that there is insufficient regulation in this area in Slovakia.

The new Payment Services Directive is a good opportunity to update the rights of consumers and Slovak users against the problems that may arise from the use of means of payment.

THE MEANS OF PROTECTING YOUR PAYMENT IN SLOVAK LEGISLATION

Although we can consider that the laws are so clear and sufficient in practice, there are many problems where one card or identification information of a card is misused and consumers were not harmed by an illegal withdrawal of money from your account bank. In most cases the banks / card issuers are unwilling to accept the consumer's point of view or arguments and usually state that the consumer caused the problem and that the card issuer has not committed a fault – mostly in cases where the perpetrator of the fraud is unknown, which is very common

The misuse of credit cards are regulated by Payment Systems decree number 510/2002, effective from August 31, 2002. § 25 - obligations and consumer complaints against the bank / card issuer in case of misuse of the card.

They are also relevant provisions in the Penal Code, Act 300/2005, § 219 - on counterfeiting and unauthorized use of half of electronic payments and payment cards of other people (the basic penalty is 1 to 5 years of imprisonment and 5 to 12 years in special cases when it causes great damage, such as belonging to adangerous organized group).

As for transfers, we find only the Payment Systems decree number 510/2002, effective from August 31, 2002, § § 3-11 for domestic transfers and § § 12 -20 for international transfers. Sin embargo, no contiene ninguna provisión específica para los Consumidores. However, it does not contain specific provision for consumers

For online payments, money transfers that are linked to information technology (IT systems and the Internet) are the Payment Systems Act number 510/2002, § § 21-24, effective since August 31, 2002. However, due to rapid developments in this sector it can be seen that this rule is slightly updated and it is necessary to establish new laws.

EXPERIENCE OF FINANCIAL INSTITUTIONS IN THE FIGHT AGAINST FRAUD

The international supermarket chain Tesco in Slovak Republic deals with concrete data on the means of payment fraud in Slovakia, in addition to having practical experience on the credit card payments in Slovakia from the entrance of Tesco in the Slovak market, in 1996.

Specifically, 1.8 million customers make their payments in the establishments of TESCO in Slovakia monthly, with an annual total of 93 million transactions in 2008. Overall, card payments account for 26% of all payments made by customers of Tesco. Since 1996, the same moment that Tesco was established in Slovakia, it is possible to pay by credit card at all TESCO hypermarkets.

The main problems faced by TESCO in the means of payment other than cash are:

The amount receivable is charged more than once on the customer's current account

If the problem is identified immediately by the client (for example, a mechanism for sms alerts) computer systems TESCO immediately returned (after confirming the error) the amount incorrectly charged to the customer's account

In the problem is discovered later by the client, the system of payments control during the closure of cashiers will reveal the problem and start on its own procedure to contact with the customer´s financial institution to resolve the problem .

The recovery of the amount is not possible

This problem can be motivated because you used a wrong code 3 times, because the signature of receipt is suspicious or does not match the cardholder's identity or where the client does not match the identity of the cardholder (for example, when the wife pays husband's with the card or vice versa)

UNICREDIT The bank operates in Slovakia and other 21 countries of Central and Eastern Europe. The main criminal activities that UNICREDIT security of means of payment have identified are misuse of credit cards by a third person who has removed from the holder, card abuse by family members of the holder, systems susceptible to fraud by the issuer of the card skimming and phishing..

In Slovakia, cards incorporate several security mechanisms to hinder counterfeiting, as the establishment of standards in terms of size, the introduction of kinegramas or holograms on the card, the use of special materials in the part where the holder must sign the card, the introduction of elements that can only be seen under ultraviolet light, using various protective elements and the establishment of a limited time for the validity of the card.

The protection of electronic data also occurs in the magnetic stripe and chip cards and it is even wanted to be increases in contactless payment cards and virtual cards.

The skimming is a type of fraud in common means of payment especially in Slovakia, compared to other types of fraud with much more sophisticated technology that are present in other countries where card usage is much more widespread and, therefore, in a more mature stage in the use of means of payment. The skimming is basically a copy of the magnetic stripe of cards, although they may be variants of the same as copying card details on computers, the illegally copied data from your computer to a blank card and the consequent use of these created cards for illegal financial transactions.

The illegal production and use of electronic means of payment or cards is punishable by the Penal Code, article 219, with sentences of 1 to 5 years.

THE EXPERIENCE OF THE SECURITY FORCES

The Slovak police highlights the following frauds as the most frequent in Slovakia:

- Stolen card / fraudulent transactions at ATMs or in shops
- "skimming" or copying banda magnate ATM cards
- "skimming" in shops
- Cards not received by the holder
- Various types of electronic fraud, such as pharming, phishing, etc.. (without the presence of the card).

Regarding the current situation and trends in the Slovak Republic are the following issues:

- There is a continuous increase over time in such crimes.
- The modus operandi is increasingly specializing, introduciong improvements in their techniques to make it more difficult for the police and security companies
- It will be a concentration of criminals by country or nationality (specialization of mafias)
- It is necessary to monitor risk in real time continuously (24 hours 7days a week)
- There are new types of cards that increase the safety of systems against the attack of thirds.

The hybrid cards are cards that include a chip to use the same non-contact, in addition to a second chip for using with EMV chip technology. The contactless chip is typically used in applications requiring fast transactions (eg, transportation), while the contact chip is typically used in applications requiring high security such as banking.

We also find dual interface cards, similar to the hybrid card (the card that provides two interfaces, with and without contact). The most important difference is that the dual interface card has a single integrated circuit.

There have been a number of factors and issues that have been determinative of the status of fraud means of payment other than cash in Slovakia

- Location of Slovakia into the Schengen Area.
- Entry of Slovakia into the European Union (acceleration of the process of convergence with the European countries of the EU).
- Economic stability and improving the quality of life of the Slovaks.
- Increased tourism.
- Slovak market opening.
- Specification of the Criminal Code.
- Cooperation between different financial institutions (monitoring of transfers, increased security at cash point terminals ventay, cooperation between banks and police, hybrid cards, bank regulation, etc.).

CONCLUSIONS

- It´s a need to increase public awareness and participation in the fight against fraud in means of payment, both in countries where its use is more advanced and in others where it is now widespread use, such as Slovakia
- The introduction of new safety methods and marketing of new payment instruments more sophisticated (eg, the case of hybrid cards) may be beneficial in establishing a greater difficulty in breaking the protection that the various security mecanisms carry on instruments for payment.
- Security on cash points should be increases by establishing some forms of regulation for financial institutions in this respect, standards and minimum requirements for the safety of cash points and forcing to check the dual set of cards.

CONSUMERS AGAINST THE FRAUD IN MEANS OF PAYMENT

- Organised byr ADICAE
- 3 April 2009
- Local Congress Palace of Madrid

Participants:

D. Piet Lakeman,
Fraud Management Senior Manager (Visa Europa)

D. Emilio Castellote,
Product Marketing Director, Panda Security

D. Miguel de Bas Sotelo,
OPTIMAWEB Executive Adviser, ANEI representative (National Association of Companies on the Internet)

Angel Barbero,
SAFETYPAYCounselor

Gabriel Agatiello,
Trend Micro representative.

CONSUMERS AGAINST THE FRAUD IN MEANS OF PAYMENT

PRIVATE SECTOR PROPOSALS

Visa Europe's role in fighting fraud means of payment

Visa Europe is part of Visa's global network. It is an association of 4,600 European financial institutions, together with the influence and oversee the direction of the company, its systems and operations. Visa Europe is a privately owned company. The headquarters of Visa Europe in London, with offices in Athens, Bucharest, Brussels, Istanbul, Stockholm, Frankfurt, Lisbon, Madrid, Milan, Paris and Warsaw.

The structure of the European market for payment systems is changing at present. European banks have traditionally functioned as a mosaic of different national payment infrastructures. However, it is universally accepted that all (financial institutions, retailers, consumers and the economy in general) would benefit from a European payments market is more open and consistent.

The European Commission has outlined its vision of an internal market for payments. And there are two other initiatives underway that are helping to turn this vision into reality: The European Central Bank has called on European banks to create a Single Euro Payments Area (SEPA)

El Banco Central Europeo ha invitado a los bancos europeos a crear una Zona Única de Pagos en Euros (SEPA)

The financial services industry has created the European Payments Council to agree a common response, that has ended under SEPA for cards (SEPA Cards Framework - SCF).

Security measures favourable to consumers

Requiring standards to its members

An industry standard established by the means of payment PCI DSS. It is a comprehensive set of requirements designed to improve data security for payment of the account established. PCI DSS includes 12 key requirements for organizations that accept or process card payments:

- Install and maintain a firewall configuration to protect data
- Do not use default passwords provided by the supplier or other security parameters
- Protect the data stored
- Encrypt transmission of data or sensitive information holders
- Use and regularly update anti-virus program
- Develop and maintain more secure applications and systems
- Restrict access to only to essential data
- Assign a unique ID for each person with computer access to the same
- Restrict physical access to data owners
- Locate and monitor all access to network resources and information
- Experiment with your regular security systems and processes
- Maintain a specific policy for information security

The migration to EMV chip technology has been spearheaded by Visa Europe, adding a new element of protection against fraud.

VISA and the protection against Card-not-present fraud.

When a Visa card is not present during a transaction (electronic commerce, payment by mobile phone or mail), there are used a wide variety of verification services to protect and authenticate the transaction.

he three main solutions proposed to authenticate these transactions are:

Security Code (CVV)

It's called the security code on the card. This is the security code of three numbers on the back of every Visa card on the signature panel or your right.

ADICAE Rating: This code can be used against you in the event of physical theft of the card as the offender would have access to the numbers and codes..

Verified by Visa

Security solution for electronic commerce. It is a system of authentication of the identity of the owner password protected which is designed to counter online fraud.

ADICAE Rating: Vulnerable if your computer has trojans, spy-ware or before final action by a hacker.

The verification of the address (AVS)

This system verifies the billing address of the holder. It is now used only by businesses in the United Kingdom.

MEASURES IN THE FIGHT AGAINST CYBERCRIME

The experience of Panda and Trend Micro

The biggest problem with regard to transactions on-line is associated with two very common scams: "Phising 2.0 (personalised computer fraud) and “Financial spam” (frauds where they try to persuade us to do somenthing with a rpomise o high reward)

There were Highlighted as specially dangerous factors:

-Overconfidence, and a lack of consumer information in these scams over the Internet (study conducted by the FBI)

-Complexity of the latest viruses that are being used to commit fraud, which are apparently harmless, ie, installed on your computer without causing any damage is more, to another is not remove the virus and destroy the site or operating system (and Him) download Windows updates automatically to protect the system, it is difficult to detect by the user..

Self Regulation ¿= Security for users?

Creation of confidence standards

The ANEI (National Association of Companies on the Internet) has created an online trust seal, Optima Web. This is a seal of quality (like the famous ISO 9000 and ISO 14000), ensures the protection of consumers in all areas of the Internet, from trade to on-line child protection. So when you see the web page you are viewing has the best web seal, it is certain that the company behind this site complies with the standards that establishes quality seal. It also includes ways of conflict resolution such as arbitration on-line or a third party mediates in the resolution. He explained that by 2010 it is expected that up.

Safetypay

The main problems that consumers in their purchases over the Internet has changed throughout the years, the queen and 2005 the major concerns of consumers that the products were arriving damaged, logistical problems, however in 2007 the problems which is the consumer and are not problems related to logistics, but rather with issues such as the products purchased do not match those offered on the website, problems with your return, and problems when downloading.

Through various statistics it was stated that the demand for Internet purchases would be further increased if they also could pay securely, as it is one of the issues of greatest concern to consumers to buy through this means.

ADICAE's experience in the protection of the rights of users of means of payment

ADICAE denounces the lack of protection for users in their transactions via "Internet Banking". The providers of this services prefer to hide these serious problems rather than invest in proper security systems.

One of the issues raised is that there are many means of payment available to the users credit card, bank electronic transfers, mobile payments, electronic money ... but, Are they really safe? Since ADICAE manifested serious doubts. .

Entities only invest in their own security and not in their clients who seek to impose any liability for fraud. In most cases, consumers haven't even a copy of the signed contract, which creates many practical problems facing the courts, because they are unaware of the terms of the contract prior to the filing of the claim. The solution to such disputes must be out-of.court, and necessarily should articulate a more effective pre-litigation

Banks and savings banks not only should proceed immediately to provide improvements in security measures, which currently pass through the implantation of the chip, but should articulate cheaper but other mechanisms which may be equally effective. For example, sending an immediate confirmation message to the mobile phone each time you make a purchase with the card, something that had already begun to do some entities, which obviously does not relieve the consumers to check bank statements more carefully and often.

ADICAE urges immediate eradication of all the contracts clauses by which the institutions limit their liability in these cases, because many are subject to these terms, is clearly abusive, to avoid responding to its customers. The disregard of banking services seems to forget that consumers take part in many cases of fraud, responding to the first 150 euros if the fraudulent purchases have been loaded before the client notifies the customer service requesting cancellation because once canceled customer should not be charging any amount. But undoubtedly the most serious are the frequent occasions on which banks and ignores the claims of affected customers.

CONSUMER PROBLEMS RELATED TO THE MEANS OF PAYMENT

ADICAE proposals for resolution

Problems in means of payment

Technical problems arising from normal operation of the means of payment (fraud Consumer expectations for the use of means of payment)

ADICAE proposed solution:

- Adequate controls and continuous investment by institutions issuing means of payment and credit institutions. Need to establish legally enforceable minimum investment
- Prudential controls
- Warning System: Rapid and continuous communication between entities stations, banks and consumer associations to communicate faults detected
- Regulation setting out the commitments of the issuing entities avoid liability clauses exoneratorias from entities (Control of contracts from financial institutions).
- Campaigns to inform consumers
- Mechanisms of dispute resolution and effective participation of consumer associations.

Problems arising from criminal activities (criminal fraud in means of payment)

ADICAE proposed solution:

- Adequate controls and continuous investment by institutions issuing means of payment and credit institutions. Need to establish legally enforceable minimum investment
- Prudential controls
- Warning System: Rapid and continuous communication between entities stations, banks, police and consumer associations to communicate and criminal proceedings risks identified.
- Regulatory clauses to avoid liability exoneratorias by institutions.
- Mechanisms of dispute resolution and effective participation of consumer associations.

PART 3

Conclusions and proposals from ADICAE

This project represents an innovation in the fight against fraud in the means of payment and other economic crimes which harm the general interests of consumers. Traditionally, in the various initiatives undertaken by various institutions (and especially by the European Commission) consumers and users have been ignored, excluding from the legislative process to their legal representatives, who are the consumers' associations.

In spite of this fact, the European Commission, aware of the growing problems associated with the use of means of payment other than cash, has admitted several times that it is necessary to involve consumer associations in the fight against such crimes.

For example, in the Commission Communication to the Council, the European Parliament, the Economic and Social Committee and Europol - A new Plan of Action of the EU (2004 - 2007) to prevent fraud on the means of payment other than cash (SEC (2004) 1264) states that the citizens of the European Union should have a more abundant and clearer scope about the security of payments. There should be prepared specific initiatives aimed to prevent counterfeiting of identity in the EU. The dissemination of information on existing educational material is still limited among consumer associations, particulary in cross-border disputes.

It is still necessary to define best practices respect to the guides for consumers, highlighting the risks associated with cashless means of payment and indicating the best ways to avoid them.

Specifically, the prevention of fraud and counterfeiting of means of payment has been delineated as a priority measure under the various Action Plans on Financial Services undertaken by the European Commission; this is because efficient and user-friendly non-cash payments, widely accepted, reliable and available at a low relative cost are essential to a modern economy and an integrated single market.

Taking into account the severity and development of fraud in means of payment it is necessary to operate from all sectors in a coordinated way. The level of cross-border fraud is higher than the national fraud; in the case of payment cards, it is several times higher than the overall rate of fraud in the EU. The fraud has been increasing in all forms, but especially in the case of remote payment transactions, especially via the Internet. While sales of electronic commerce in recent years have exceeded the most favorable, its potential is being hampered by the lack of consumer confidence in the security of payment transactions made through Internet. It is therefore necessary to address the action from a distinctly European perspective.

Consumers and their role in the eradication of fraud in payment means

The various plans of action against fraud by the European Commission noted the need for increased attention on fraud in means of payment and in this respect are of paramount importance, in addition to other actions, some preventive measures to combat fraud and forgery of means of payment. Besides using a principle of caution and special protection for consumers, for new payment methods, more and more technology is needed to create a counterbalance and dialogue with companies.

The actions that are going to fight against the problem of fraud in cashless means of payment from the perspective of legitimate associations representing consumers and highlight the importance of consumer involvement in the fight against fraud, since they represent the weakest link in the chain of fraud. Any decision affecting the consumers must be consulted and agreed with them.

The actions that are going to fight against the problem of fraud in cashless means of payment from the perspective of legitimate associations representing consumers and highlight the importance of consumer involvement in the fight against fraud, since they represent the weakest link in the chain of fraud. Any decision affecting the consumers must be consulted and agreed with them.

As a consumer association, we should encourage the creation of a common front of consumers in this area. ADICAE intends to continue with the general objectives that motivated the launching of this project, as an Association that specializes in consumer financial issues this is their greatest concern.

ADICAE proposals to combat fraud in payment means

Establishment of the Center of Supervision of Fraud in Cashless Means of Payment:

It would be useful to establish a collaborative agreement between the parties to create a mechanism to establish a permanent dialogue between all interested parties (payment card systems, banks, payment systems, banking associations, equipment manufacturers and cards payment, Europol, Interpol, public authorities, including agencies of enforcement, retail, consumers, network operators) to implement the proposed partnership approach and ensure maximum effectiveness in combating fraud and counterfeiting in payment in addition to further actions.

Functioning of the Center:

- Fraud involving experts from each sector and country.

- Work in sub - groups, led by an organized group.

- The General Board of the Center will meet at least twice a year.

- There will be created various sub - working groups to control and supervise the different areas

Objectives of the Observatory:

Collaborate with the payment systems to review their practices and procedures on an ongoing basis and modify or discontinue those that may promote fraudulent behavior. Collaborate with the payment industry to establish best practices regarding teaching materials for retailers and consumers where preparing new materials becomes necessary.

Assist in informing retailers about the status of payment instruments presented for acceptance and advice on how to deal with suspicious transactions. Collaborate with consumer associations in developing guidance on new areas of risk (eg, online payments), and fraudulent behavior by encouraging consumers to take reasonable steps to prevent fraud

Assist in implementing a single telephone number for all EU consumers to facilitate the notification of the loss or theft of a payment instrument, or at least one phone number for all issuers of each Member State.

Assist in the review, and proposed implementation of legal guarantees and obligations of the parties relating to fraud and counterfeiting of means of paymen.

The Commission will organize a meeting with consumer organizations and other stakeholders to discuss ways to develop and promote consumer education about the risks associated with different payment mechanisms and the best way to avoid these risks.

Creating a trust logo on European means of payment

The logo of confidence, in line with other initiatives in particular of a business (rather unsuccessful so far) is based on the following elements::

- A set of ethical standards in a Code of Ethics should stablish, in particular, the regime of liability of operators in relation to the various European recommendation that, in general, are not respected by means of payment providers and Financial entities..

- A mechanism to implement such rules should be responsible for resolving disputes and grievances that arise. It should also set up an Arbitration Board for a special means of payment, which would act after mediation attempt by the consumer associations

- Own a body, responsible for the processing and procedures as well as the daily management of the system of self and trust, and which will address the claims brought by alleged breaches of the rules of this Code.

- And a trust mark that identifies companies adhering to this system of self-regulation, which could display their information and promotional material companies that are part of this system of self as distinct from its membership.

Cooperation between states

International cooperation among the stakeholders as the best way to fight against fraud.

It has been stated that in order to fight against crimes which are composed of diverse cross-border law infractions national police authorities must cooperate among themselves, with the supervision of a supranational body such as in this case is Europol.

So, in other issues like the legislative processes or the creation of educational policies for consumers, which contribute to the effective prevention of these kinds of crimes, the cooperation among the diverse stakeholders must be exist in the same way.

For more conclusions and technical advises look for other publications of ADICAE´s project.