

Preventing payment fraud in Europe

Next FPEG Meeting: 19 December 2007

Fpeg plenary. The next meeting of the FPEG will take place on 19 December 2007. The meeting will focus on the **presentation of the final report on the study on user identification methods in card payments, e-payments and m-payments**. The objective of this study is to analyse current and prospective user verification methods in this kind of payments by providing an assessment of their security features, but also of their user-friendliness. The study also analyses possible regulatory, contractual or commercial barriers to the use of best technologies, whether available or prospective.

The agenda of the meeting will be made available at the FPEG website beginning of December.

http://ec.europa.eu/internal_market/fpeg/index_en.htm

Portuguese Presidency: Conference on Identity Theft/Fraud; 7-9 November 2007

The Portuguese Presidency of the European Union is organising on 7-9 November a **Conference on Identity Theft/Fraud: the Logistics for Organised Crime**. This conference is aimed at fostering the exchange of experiences as well as an integrated and updated approach on fraud and theft of identity, while highlighting its relevance in the current state of affairs from the criminal point of view. Special account shall also be given to the fact that most contacts, contracts and transactions are made via Internet and that the increasingly modern and simplified acts of administrations have lead to procedural de-materialization and allowed personal data, retrieved for different purposes, to be recorded and managed in computer databases.

The conference also seeks to complement similar initiatives, primarily those adopted within the European Union framework, and to further harmonize the measures and approaches in the field, forecasting agreement upon operative recommendations and **follow-up activities** towards a common strategy to the prevention of and fighting against some of the identified problems.

The effects of identity theft/fraud in the financial sector will be addressed in the Conference.

Further information at:

www.idfraudconference-pt2007.org

FPEG Report on Identity Theft/Fraud

The FPEG Report on Identity Theft/Fraud was disclosed at the end of October 2007, following its discussion at the June meeting and the subsequent amendments introduced. The aim of this non-exhaustive paper is to provide an **overview of the identity theft/fraud problem in the financial sector** in particular in the payment and retail banking areas, outlining the main risks and the vulnerabilities all along the identity chain in the financial system.

The misuse of personal data to impersonate somebody else and abuse of his/her banking/financial services facilities is a **growing concern** in developed societies. In some EU Member States identity theft/fraud is the fastest growing type of financial fraud. In its Action Plan of 2004 on payment fraud prevention, the European Commission pointed at this problem and underlined the need to strengthen businesses and consumers confidence regarding non-cash means of payment, in particular those used in non-face to face situations.

The first difficulty is to define the **scope of the problem** as there is no clear common definition of what should be understood by identity theft or identity fraud and also measuring it. Indeed, the consequences for the victims vary.

Zero fraud does not exist. Indeed, there are vulnerabilities in the identity chain but also responses to those vulnerabilities that can help in reducing current identity theft/fraud levels in the financial system: first and foremost, **preventive measures**. Preventative measures, however, are not the responsibility of an isolated actor within the identity chain, but of all actors. Joint cooperation by stakeholders is therefore needed to enhance security. No one aspect of the identity chain can be managed in isolation.

There are a number of preventative measures which are applied by the **financial system actors** in the three main phases of the business/commercial relationship: enrolment, system use and termination. Risk and vulnerabilities are different (account takeover, false application etc), as well as the responses. And there is scope for improvement. Current solutions for authenticating customers have limitations and may be relatively insecure. Therefore, there are a number of other measures that could be used to confirm the "contractual identity" of the client. Concerning phishing (and similar scams such as pharming), customer education is important so as to enable him to recognise false messages. Customers should indeed be more responsible for their actions in the internet world.

Public authorities are also responsible for preventing identity theft/fraud. There are several best practices applied by some authorities. Generalisation of the best practices described would be welcomed by stakeholders.

In addition, the fight against identity theft/fraud cannot be complete without strict prosecution and **traditional law enforcement measures**. Identity theft/fraud in the payment area is normally not a criminal offence on its own, but an enabler for other offences. As a result, there is a vast disparity of penalties applied in Europe. Stakeholders have the perception that those penalties are generally too low to be dissuasive. A certain harmonisation of EU criminal legislation in this regard seems to be supported by stakeholders.

The report concludes that,

- (1) It is important to maintain the integrity of the identity chain. Currently the weakest links of the chain are: the customer's personal computer (customers should be aware of it and be motivated to secure their own environment); the Internet Service Providers; the data storage service providers acting as third parties, as well as the databases operated by merchants and public authorities. In this chain, the responsibility should be taken up by all the parties to the chain, within their own limitations.
- (2) Identity theft/fraud does not only affect the financial sector. Its effects go beyond. Other stakeholders should be associated to this fight.
- (3) It is of great importance to make available educational tools for "weak" parties (citizens and SMEs) in relation to the use of the Internet.
- (4) Technology is part of the solution but will not be the only solution.
- (5) Caring for victims make sense as it should provide for improved trust.

The report has been made available as background material to the Portuguese Presidency Conference on Identity Theft/Fraud.

The report is available at:

http://ec.europa.eu/internal_market/fpeg/index_en.htm

Cybercrime: expert crime meeting of 15/16 November 2007

An expert meeting on cyber crime will be organised by DG Justice Freedom and Security of the European Commission on **15-16 November**. The main objective of the meeting is to have an open and informal discussion on the needs for actions to fight cyber crime at EU level (as a follow-up to the cyber crime communication, adopted on 22 May 2007 – see **FPEG News**n°4). The meeting will consist of three sessions. The first session will be open to Member States law enforcement representatives only. The other two sessions will also include a number of participants from international organisations (OSCE, G 8 Roma/Lyon Group, Interpol, Council of Europe etc.) and private companies. Participation will be on invitation only. The two public-private sessions will concentrate on the specific issues of fight against child sexual abuse material and fight against attacks on information systems.

http://ec.europa.eu/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm

Background information: the FPEG and the prevention of payment fraud in Europe

The EU Action Plan. In October 2004 the Commission issued an **Action Plan 2004-2007 of non-legislative measures to prevent fraud and counterfeiting of non-cash means of payments**, with a view to foster a more coherent approach to fraud prevention. This Action Plan builds on a previous one of 2001. It will complement the Commission's recent proposal for a directive on payment services in the internal market (the so-called "New Legal Framework for Payments", December 2005) in underpinning the creation of a Single Payment Area in the EU. It also complements the banking industry initiatives to establish a single Euro payments area (SEPA) aiming to enable European citizens to make payments in the Euro area as securely, quickly and efficiently as payments within national borders. SEPA should be in place by 2010. Finally, the Action Plan should notably continue and further strengthen the existing initiatives to prevent fraud and contribute to maintain and increase confidence in payments.

The FPEG. A **Fraud Prevention Expert Group** (FPEG) was established under those Action Plans. This experts' group at EU level includes representatives of all parties involved in fraud prevention: i.e. national and EU payment schemes, banks, national public authorities, European and international law enforcement agencies (e.g. Europol, Interpol) retailers, consumer groups, network operators etc. The FPEG provides for a platform where stakeholders can effectively exchange information and best practice to prevent fraud. It contributes to intensify cooperation between interested parties, especially at cross-border level. It provides advice to the Commission.

How is the work of the FPEG organised? The FPEG meets twice a year. The FPEG is chaired by the Commission, but a **steering group** of FPEG members helps in the preparation of the work of the FPEG and supervise the sub-groups activities. Several **subgroups** have been created. Reports have been made by the subgroups dealing with Security Evaluation Procedures, ATM and POS Security, Identity Theft/Fraud and Data Management. The subgroups may not necessarily be chaired by the Commission. The secretariat of the FPEG and the subgroups is provided by the Commission.

More Information

More information is available at the website of the **FPEG**: http://europa.eu.int/comm/internal_market/payments/fraud/fpeg/index_en.htm

You may contact the **FPEG secretariat** through the e-mail address provided in the website.

Disclaimer

The views expressed in **FPEG News** are purely those of the FPEG and may not in any circumstances be regarded as stating an official position of the European Commission.