COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.4.2008
SEC(2008) 511

COMMISSION STAFF WORKING DOCUMENT

Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan

Contents

EXECUTIVE SUMMARY

Fraud against means of payment (**payment fraud**) remains a threat to the success of the internal market for payments. Payment fraud affects the consumer confidence in non-cash means of payment and ultimately the real economy. In 2004, the European Commission presented a second Action Plan. Its purpose was to foster a more coherent approach to fraud prevention. This report presents the implementation of this Action Plan for its duration, 2004-2007. Additionally, it provides an overview of the broader context on the prevention of and the fight against payment fraud.

The **Action Plan** measures have been implemented in cooperation with the key stakeholders, through the Fraud Prevention Expert Group (FPEG). These measures have focused on payment cards, which is the most common means of payment for cross-border retail transactions. The FPEG has prepared reports in response to developments, such as: ATM security, data management for prevention purposes, harmonisation of security evaluation procedures and identity theft. Awareness actions have also been undertaken, notably in 2006 a seminar on prevention of payment fraud with countries aiming to join the EU and a high level conference on identity theft and payment fraud. Europol, in cooperation with the payments industry and in some cases with the financial support of the Commission, continued to provide specialised training to national law enforcement authorities. Other supporting measures included the creation of a database of original and counterfeit identity documents and facilitating the possible implementation of a single phone number in the EU for the notification of lost and stolen payment instruments. Finally, transparency about the Action Plan work is provided through a website dedicated to the FPEG activities.

In the 2004-2007 period, new **European legislation in the financial services area** has been enacted. This legislation contains provisions which directly or indirectly address the prevention of payment fraud. In the first place, the directive on the prevention of money laundering (2005) requires the implementation of a sound "know your customer" policy by financial institutions. Additionally, the new Directive on payment services (2007) contains specific rules aimed at reducing the risks and consequences of unauthorised payment transactions. This new legislation contributes to the creation of a more robust legal environment at EU level in this area.

Guaranteeing high standards of security is one of the aims of the work leading to the creation of the **Single Euro Payments Area (SEPA)**. The European payments industry is working on the harmonization of security requirements, in particular regarding cards. The new SEPA Cards Framework attaches high importance to fraud prevention and requires any adhering card scheme to support fraud prevention activities in accordance with the European Payments Council (EPC) resolutions on card fraud. The European Central Bank policy regarding the oversight framework for card schemes will also contribute to reinforcing safety of the payment cards, also in relation to securing the initiation and operation of transactions.

In addition to the legislative developments, several initiatives regarding the prevention of payment fraud have been undertaken, in most cases directly by the payment industry. Regarding face to face situations (in payment cards), the movement towards the EMV **chip and PIN** technology as transaction authentication method in payment cards has largely contributed to the reduction in fraud associated with lost and stolen cards in Europe. Also in relation to lost and stolen payment instruments, the Commission adopted in 2007 a decision reserving the whole range of phone numbers beginning with "116" to be used for "harmonised

services of social value". This type of number could be used for **card stop services** if the criteria for the allocation of the numbers are fulfilled.

However, **skimming fraud** has increased in recent years. In this situation, the magnetic stripe (not the chip) of cards is copied in payment terminals or, more often, in ATMs or unattended payment terminals (for example those in petrol stations). The copied data (in some cases the PIN code is also captured) are used for the production of counterfeit cards which are then either used in non-EMV terminals (in Europe or in countries where the EMV technology has not been implemented) or for non-face to face payments (e.g. mostly Internet transactions). The payment industry, through the EPC and the EAST Group are adopting preventive measures to counter this phenomenon. An FPEG report provides an overview of these measures.

The EMV success has resulted in an overall decrease in card fraud losses, but at the same time generated a *de facto* shift of payment card fraud towards remote (e.g. non-face to face) situations, mostly in the Internet environment: the so-called **card-not-present fraud**. This type of fraud is increasing in Europe and is considered to constitute the highest threat for payment cards. In reaction to this threat, the EPC recommends ensuring the use of the card security codes as from January 2008 and the payment industry is providing incentives to merchants and cardholders for the use of enhanced secure verification methods in internet payments (mostly based on the 3D Secure market standard). Regarding **e-banking fraud** (which includes phishing), banks are progressively moving to enhanced customer/transaction authentication methods. An insight on user authentication methods in cashless payments is provided in a study conducted for the Commission in 2007. Fraud in non-face to face situations is related to identity theft/fraud and cybercrime (see below).

The preventive activity of payment service providers also relies on **fraud detection tools** or monitoring databases, as recognised in the payment services directive. However, the desire by the payment industry to pool data between payment instrument issuers (for instance at card scheme level in a SEPA wide area) poses challenges as far as data protection is concerned. The FPEG discussed the data sharing issue in different meetings and a report on the limits to the sharing of personal data for fraud prevention purposes was prepared in December 2006.

Prosecuting fraud should complement the preventive measures. EU legislation is this area was adopted in 2001 and is implemented in most EU Member States. While the deterrent effect of criminal penalties for payment fraud offences should be a key element of the fight against fraud, some stakeholders have the perception that the penalties applied in practice at national level in this field are generally too low to be dissuasive. There are additional practical difficulties for the law enforcement authorities to ensure a fast reaction against fraud. Particular problems include finding enough evidence to prove the criminal conduct (also because of the high technology dimension of most fraudulent conduct) and the cross-border dimension of many attacks. Member States have reacted by creating/reinforcing specialised police units to deal with cybercrime. Additionally, cross-border police and judicial cooperation and assistance have been reinforced, notably through the Joint Investigations Team network sponsored by Europol and Eurojust, with encouraging results. In the last years Europol provided specialised training, in cooperation with payment card schemes, to national law enforcement authorities on operational aspects of payment card fraud, in particular on skimming and hi-tech payment card crime over the Internet. This specialised training improves the expertise and the financial investigation capacity of the law enforcement authorities in this field.

Some challenges remain. First, increasing the **understanding of the nature and the extent of the problem** is of primary importance in order to evaluate the risks, implement the appropriate measures to counter fraud and measure their effectiveness. The EPC is developing an anti-fraud database that should be operational in 2008 and would integrate aggregated statistics on fraud covering both national and SEPA-wide transactions. The Commission has also addressed the need to improve the statistics in the criminal area as regards crimes and criminal prosecution by launching an ambitious action plan 2006-2010 on developing an EU strategy to measure crime and criminal justice.

Secondly, payment fraud is a moving target. New threats appear, in particular **identity theft/fraud** and, more generally, **cyber crime** (which includes many of the identity theft/fraud typologies). Community responses to these new threats have been numerous in recent years, both at regulatory level and by raising greater awareness. Regarding identity theft, this has included, *inter alia*, the high level conference on identity theft/fraud organised by the Commission in 2006, which has resulted in some follow up actions, or FPEG report. The identity theft/fraud problem also raises issues from the wider perspective of identity management. The Commission has funded important research projects in this area through the 6th Framework Research Programme (FP6) and has launched a new set of information and communication technologies security projects as part of 7th Framework Research Programme (FP7, 2007-2013). Regarding cybercrime, the Commission adopted a communication in 2007 setting out its priorities in this area. In addition, the EU institutions continue to develop policy with a view to improving network and information security, which continues to pose challenging problems. In 2005 the Council adopted a framework decision requesting Member States to criminalise certain attacks against information systems. In 2006 the Commission also presented a specific communication on network and information security identifying risks and possible work streams for the future. The establishment of ENISA (European Network and Information Security Agency) in 2004 has also been a major step forward in the EU's efforts to respond to the challenges relating to network and information security. The regulatory framework for electronic communications, which includes security-related provisions, is currently under review and in 2007 the Commission proposed modifications to three directives, including on security issues. In a communication of 2007, the Commission is also promoting data protection by privacy enhancing technologies.

Finally, fraud, even if it affects a minority of users, undermines the general **confidence in payments systems**. A study conducted for the Commission in 2007 shows that user trust in certain authentication methods for cashless payments could be improved. Maintaining or enhancing user confidence does not necessarily require new legislation but rather the commitment of the parties involved to achieve this goal. Increasing public awareness and education to enhance trust, and also to avoid the pitfalls of payment fraud, is important in this context. In the light of the increasing cyber crime attacks and the development of cashless payments on line, this also requires trusting the information society in general.

The **work conducted in 2004-2007** shows that while it is important to ensure the security of means of payment and payment systems, it is also important to improve consumer confidence and trust. The new legal framework for payments, including the "know your customer" obligations, as well as the development of SEPA by industry, should provide a good basis for increasing both security and trust. Additionally, the measures adopted by the Commission, beyond the Action Plan, in relation to the prevention of and fight against identity theft/fraud and cyber crime, should also contribute to those goals.

1. INTRODUCTION

Fraud against means of payment (payment fraud) remains a threat for the success of the internal market for payments. For instance, if one looks only at payment cards, there are 10 million fraudulent transactions in the SEPA area per year, affecting 500 000 merchants, representing roughly €1 Billion losses[1]. This threat may affect the consumer confidence in non-cash means of payment and ultimately the real economy[2]. In this context, rapid technological developments and criminals' adaptation to a fast changing environment make the prevention of and the fight against payment fraud particularly challenging.

In 2004 the European Commission presented an Action Plan[3] with a view to fostering a more coherent approach to fraud prevention in the 2004-2007 period (hereinafter, the 2004-2007 Action Plan). The 2004-2007 Action Plan consisted of non-legislative measures and built on a previous plan of 2001[4]. This report will first describe the main initiatives undertaken in the context of the 2004-2007 Action Plan (section 2).

In addition, this report will provide an overview of the broader context on the prevention of and the fight against payment fraud. Thus, this report will present the legislative evolution in the financial area affecting the prevention of payment fraud as well as the launching of the banking industry initiative to progressively establish a Single Euro Payments Area (SEPA), starting in January 2008 (see section 3). It will also describe the state of the play regarding preventive measures (section 4); the developments at EU level regarding the prosecution of payment fraud (section 5); and the main work undertaken by the Commission in relation to the new challenges, such as identity theft and cyber crime (section 6). Some conclusions will be presented in section 7.

2. THE IMPLEMENTATION OF THE 2004-2007 ACTION PLAN

The key principle of the 2004-2007 Action Plan work was cooperation among stakeholders: e.g. the prevention of fraud is more effective if implemented in partnership. This principle has guided the implementation of the Action Plan, for which the Commission has been assisted by the Fraud Prevention Experts Group – FPEG. This experts' group at EU level, established under the 2001 Action Plan, includes representatives of parties involved in fraud prevention: i.e. payment schemes, banks, law enforcement authorities, financial supervisors, retailers, consumer groups, etc. The FPEG provides a platform where stakeholders can effectively exchange information and best practice to prevent fraud. It thus contributes to intensifying cooperation between interested parties, especially at cross-border level.

---

1 Presentation of the EPC Card Fraud Prevention Task Force at the FPEG meeting of 28 November 2006.

2 See speech by Gertrude Tumpel-Gugerell, ECB, of 21.9.2004: "[…] *if fraud becomes too high for the banking sector, banks may in the future also seek compensation from users. In addition, large-scale or spectacular fraud events in card schemes may trigger a sudden change in the payment means chosen by the public. Other means of payments may not be able to cope with sudden demand peaks or, at least, there could be important frictional costs and impact on the real economy, in particular on retail commerce. Fraud combat is a top priority. […]*"

3 Communication from the Commission of 20.10.2004, *A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment*, COM(2004)679 final.

4 Communication from the Commission of 9.2.2001, *Preventing fraud and counterfeiting of non-cash means of payments*, COM(2001)11 final.

Regarding technological and fraud developments, the work focused on payment cards, which is the most common means of payment for cross-border retail transactions as well as on the Internet. The FPEG prepared reports on two key issues: (i) harmonisation of security evaluation criteria for card payments (see section 3 below) and (ii) ATM security, including card skimming (see section 4.1 below). The Commission also published in 2007 a study on user verification methods in cashless payments (see section 6.3 below). The FPEG further undertook work with a view to facilitating the exchange of information among stakeholders for an early detection of fraud (cf. point 6 of the Action Plan). A report was prepared evaluating the implications of the personal data protection legal framework for the processing of fraud related data (see section 4.3 below).

The Commission also worked with a view to contributing to the increase in the performance of national authorities in this area. This included in particular the organisation of a seminar on prevention of payment fraud with countries aiming to join the EU, which took place on 8-9 March 2006[5]. It was attended by representatives from the public and private sectors of Bulgaria and Romania (at the time accession countries); Croatia, Turkey and the former Yugoslav Republic of Macedonia (candidate countries); Serbia, Montenegro and Bosnia Herzegovina (potential candidate countries). The aim of the seminar was to enable police officers, prosecutors and regulators from these countries to increase their knowledge and awareness of the issues related to payment fraud. It was a first step towards enhancing cooperation on payment fraud between EU Member States and these countries. Additionally, Europol, in cooperation with the payments industry and in some cases with the financial support of the Commission, continued to provide specialised training to national law enforcement authorities (see section 5 below). Finally, The Commission also organised a high level Conference in November 2006 for the benefit of national policy makers with regard to identity theft and payment fraud, one of the new challenges in the field of fraud prevention (see section 6.2 below).

Other fraud prevention measures were also completed, for instance, the creation of a database of original and counterfeit identity documents (see section 6.2 below) or the possible implementation of a single phone number in the EU for the notification of lost and stolen cards (see section 4.1 below)

In addition to the awareness raising initiatives, such as the seminar and conference in 2006, the Commission and the FPEG have provided greater transparency about the work undertaken. A website dedicated to the FPEG activities was created[6], providing access to: the FPEG reports; information on discussions held; presentations made and other related issues.

In this context, although not directly addressed in the Action Plan, the Commission has been providing financial support to some initiatives undertaken by stakeholders in relation to the prevention of and/or the fight against payment fraud. See Annex 1 for further detail.

Further detail on the main Action Plan initiatives[7] is provided in the following sections of this paper.

---

5 See Commission press release of 9.3.2006 (IP/06/290)

6 www.ec.europa.eu/internal_market/fpeg/index_en.htm

7 See Annex 2 for a list of the 2004-2007 Action Plan points and its concrete implementation.

3. IMPROVED SECURITY OF CASHLESS PAYMENTS FURTHER TO RECENT LEGISLATIVE DEVELOPMENTS AND THE LAUNCHING OF SEPA

3.1. The new legal framework at EU level for secure cashless payments

In the 2004-2007 period, new European legislation in the financial services area has been enacted containing provisions which directly or indirectly address the prevention of payment fraud. This new legislation has thus contributed to the creation of a more robust legal environment at EU level[8].

Firstly, the new directive[9] on the prevention of money laundering of 2005 has introduced more detailed obligations for financial institutions in relation to customer due diligence which at the same time are more flexible and better adapted to the level of risk involved. The implementation of a sound "know your customer" policy by financial institutions should lead to a better management of the fraud risks involved, notably regarding identity theft type of fraud (e.g. when accepting new customers) or non-face to face situations (e.g. when monitoring customers' transactions)[10]. The particular question of non-face to face transactions was examined by the Commission in 2006[11], with the identification of best practices and of possible ways forward.

Secondly, a new directive[12] on payment services in the internal market (PSD) was adopted in 2007. This directive aims at ensuring that payments within the EU – in particular credit transfer, direct debit and card payments – become as easy, efficient, and secure as domestic payments within a Member State are today. By setting up a harmonised legal framework for payments within the EU, the PSD will provide more transparency and will reinforce the rights and protection of all the users of payment services (consumers, retailers, large and small companies as well as public authorities). Several provisions of this directive directly or indirectly address payment fraud issues, in particular: (i) information requirements on the payment instruments, including on the use of the payment instrument and its personalised features (cf. Articles 42(2) and 42(5)); (ii) the authorisation of payment transactions, in order to reduce the risks and consequences of unauthorised payment transactions, including also allocation of liability between the payer and his payment service provider (cf. Articles 54 and seq.); and (iii) the processing of data for fraud prevention purposes (cf. Article 79).

---

8 Legislation in other areas also directly or indirectly addresses the issues of payment fraud prevention or prosecution. See in particular section 5 for criminal legislation and sections 4 and 6 for legislation on personal data protection or information and communication technologies.

9 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15.

10 See FPEG report on Identity Theft/Fraud (2007).

11 See Commission Staff Working Document, of 19.12.2006, on *the application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*; SEC(2006)1792.

12 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319 of 5.12.2007.

3.2. The security of payment instruments and the SEPA environment

The SEPA should enable people to make payments throughout the euro area as quickly, safely and easily as they make national payments. This calls for the removal of all technical, legal and commercial barriers between the current national payment markets. The European Payments Council (EPC), grouping the payment industry, has been working (and continues to work) to ensure the standardization of payment services and processing regarding direct debits, credit transfers and card payments. Guaranteeing high standards of security is one of the aims of this work.

In the case of payment cards, one of the action points identified in the 2004-2007 Action Plan related to the question of mutual recognition of the certification of terminals, cards and network interfaces. The FPEG prepared a report[13] on security evaluation. This report explained that the situation was characterized by a diversity of evaluation methods, a multiplicity of actors (i.e. essentially the ECB and the national central banks, the banking industry, the payment schemes, the certification bodies, the issuers, the evaluation laboratories and the manufacturers) and the absence of a harmonized legal framework at European level. The FPEG recommended intensifying efforts towards aligning security evaluation procedures, choosing a formal/neutral method of providing a sound evaluation assurance and promoting the exchange of information on attacks on payment systems to improve vulnerability analysis and penetration testing. The FPEG was of the view that the alignment of security evaluation procedures should result in significant cost reduction while guaranteeing a consistent high security level in the payment area.

In this context, the EPC is developing standard specifications for cards, terminals and networks, which would include mandatory minimum requirements as well as optional recommended specifications and/or best practice guidelines. This work is focusing on 4 domains[14] leading to 5 main initiatives/standards. Among these five initiatives, the Common Approval Scheme (CAS) project, an initiative of several European payment schemes, aims at proposals for: (a) minimum security requirements for cards and terminals ('point of interaction'); (b) a Common and Neutral security evaluation methodology; and (c) a framework for mutual recognition and type approval across SEPA[15]. This process, however, raises the issue of deciding what the EU body/authority will be for (i) the accreditation/monitoring of the laboratories in charge of evaluations; (ii) the endorsement of 'CAS' proposals and setting up the security rules for SEPA (CAS is proposing a certain level of security, which is high for cards and is yet to be finalized for points of interaction); (iii) the definition of an adequate minimum security level for all payment Schemes across SEPA; and (iv) the enforcement of this minimum security level for mutual recognition across the EU.

Additionally, the new SEPA Cards Framework[16] attaches particular importance to fraud prevention and requires any adhering card scheme to support fraud prevention activities in accordance with the EPC resolutions on card fraud. Two resolutions have been adopted so far by the EPC plenary, one in December 2003 ("Preventing and fighting fraud across Europe") and another one in March 2007 ("Preventing Card Fraud in the new SEPA environment"). The latest recommendation focuses on the prevention of the use of counterfeit cards at SEPA

---

13 FPEG, *A survey on the security evaluation procedures for the certification of payment products in the European Union*, June 2007.

14 Card-to-terminal, Terminal-to-acquirer, Acquirer-to-issuer and Certification and Approval.

15 See presentation by the EPC at the FPEG meeting of June 2007, available at the FPEG website.

16 European Payments Council, 8 March 2006, SEPA Cards Framework, version 2.0, in particular p.14.

terminals (see section 4.1), combating card-not-present fraud (see section 4.2) and the collection of statistics on card fraud (see section 6.1).

3.3. The ECB oversight framework for card schemes

The importance of fraud prevention for the efficiency of payment systems and instruments has always been underlined by the European Central Bank (ECB). This has again been highlighted in the recent announcement by the ECB when presenting its oversight framework for card schemes, which lays down Eurosystem oversight standards with regard to card payment schemes operating in the euro area[17]. The ECB emphasizes that, owing to the nature of card schemes systems, the risk of loss of reputation is greater than for other types of payment systems. Breach of reputation can have a severe impact on users' confidence in cards (see section 6.3).

These oversight standards focus on ensuring the safety and efficiency of the card payment schemes. Operational risk in this context includes the risk of fraud, since this can be defined as a wrongful or criminal deception which may lead to a financial loss for one of the parties involved in the payment process (e.g. as a result of an unauthorised debit of a cardholder account) and may reflect inadequate safety arrangements. According to the ECB, mitigation of these risks supposes appropriate measures to ensure: proper security management; protection of sensitive data or devices during manufacturing and distribution of cards; secure initiation and operation of transactions (also in the online environment); secure and reliable clearing and settlement; business continuity; and control of outsourcing[18].

4. MAIN PREVENTIVE MEASURES TO PAYMENT FRAUD

Further to the legislative developments, several initiatives regarding the prevention of payment fraud have been undertaken in recent times, in most cases directly by the payment industry. This section will present the state of play regarding preventive measures, first with regard to face to face situations (4.1), then with regard to non-face to face situations (4.2). The question of fraud detection tools will also be briefly addressed (4.3).

4.1. Face to face situations

4.1.1. EMV implementation

Face to face situations essentially concern payment cards. In recent years, the payment industry has been addressing fraud in these situations by increasing the security features of the payment instruments: e.g. the movement towards the chip and PIN technology (so called EMV[19]) as transaction authentication method in payment cards.

The EMV deployment is addressing two traditional types of fraud: the misuse of lost and stolen cards and the counterfeiting and subsequent use of counterfeit cards. The use of lost or

---

17 See ECB press release of 11 January 2008 ("Oversight Framework for Card Payment Schemes – Standards").

18 See ECB, *Oversight framework for card payment schemes – standards* (January 2008), in particular pages 7, 8, 11 and seq.

19 The EMV (Europay-Mastercard-VISA) standard is the *de facto* standard for microchips and terminals in the payment market.

stolen cards in face to face situations in Europe has substantially diminished in recent years[20] thanks to the introduction by the payment industry of the chip and PIN[21] technology: when this technology will be fully deployed, criminals will no longer be able to conduct face to face transactions in Europe based on the simple presentation of the lost or stolen card, as they would need the PIN to authenticate the transaction. The EPC recommended the implementation of the so-called EMV standard in Europe. As of end 2007, 56% of the payment cards issued by EU based banks use the EMV chip, 59% of the points of sale are capable of conducting EMV secure transactions and 72% of the ATMs in the EU are equipped with EMV technology (although there are significant country differences)[22]. Work is progressing towards full migration in time for SEPA (2010).

The main weakness of the EMV roll out is the fact that the magnetic stripe is still maintained in EMV equipped cards, essentially because cards tend to be internationally accepted and the EMV technology is not necessarily deployed in other world regions or not at the same pace. To the extent that the magnetic stripe can be counterfeited (which is not the case of the EMV chip to date), payment cards are still vulnerable.

4.1.2. Skimming fraud

The main threat at this stage is the so-called skimming fraud, which has increased in recent years[23]. In this situation, the card's magnetic stripe is copied in payment terminals or, more often, in ATMs or in unattended payment terminals (for example those in petrol stations). Criminals install handmade skimming devices on the card slot and copy the data stored in the magnetic stripe. The copied data is often remotely transmitted (in some cases in real time) to other members of the criminal group and used for the production of counterfeit cards. These cards are then either used in non-EMV terminals (either in Europe or in countries where the EMV technology has not been implemented) or for non-face to face payments (e.g. mostly Internet transactions). Additionally, in some cases, criminals are able to capture the PIN code of the cardholders when copying cards (for instance by attaching mini-cameras above the keypad in ATMs) and then are able to further use the counterfeit cards in European ATMs to withdraw cash (to the extent that non-EMV transactions may be still be accepted within the EU even if both card and terminal are EMV capable).

The FPEG produced a report in 2006 on the security issues related to ATMs and point of sale terminals, in particular in relation to skimming attacks. The report presents some recommendations, mostly addressed to the payment industry, on how to mitigate these attacks. Indeed, the payment industry is, through the EAST group[24], monitoring the skimming

---

20 See for instance the presentations of the EPC Card Fraud Prevention Task Force at the FPEG meetings of 2006 and 2007.

21 Personal identification number to be introduced in order to validate a face-to-face transaction.

22 See presentation by the EPC Card Fraud Task Force at the FPEG meeting of 19.12.2007

23 According to a press release by EAST (see following footnote) of 23 March 2007, in 2006 there were 4571 reported card skimming attacks, which resulted in total losses of just over €305 million euros. Compared to 2005 figures, there were increases of 23% in the number of attacks and 30% in the reported losses. See also the presentations of the EPC Card Fraud Prevention Task Force at the FPEG meetings of 2006 and 2007. See also Europol, *Annual Report* (2006), in particular the section on liaison bureaux activities (pages 32 and seq.).

24 European ATM Security Team (EAST). Founded in February 2004, EAST is a 'not-for-profit' organisation whose members are committed to gathering information from, and disseminating EAST outputs to, ATM deployers and networks within their countries/regions. While the main focus of EAST

threat and the security efforts in ATMs. Additionally, the EPC is currently considering recommending additional measures to counter this type of fraud, notably by improving the security features of ATMs and similar unattended payment terminals and/or establishing incentives for acquiring banks with a view to eliminating the acceptance of non-EMV transactions when both the card and the payment terminal are EMV capable[25].

In any case, lost, stolen and counterfeit cards can still be used in non-face to face situations, in particular for Internet payments and telephone orders (see section 4.2).

4.1.3. Card Stop numbers

Under the 2004-2007 Action Plan, it was foreseen to continue the discussions with a view to implementing a single telephone number in the EU for the notification by users of lost and stolen payment cards. Prompt notification of the loss or theft of a card is important for consumers as, in accordance with the recent Payment Services Directive, they cease to be liable for any fraud losses after such notification[26]. Indeed, this directive also contains an obligation for card payment users to notify the issuing banks of any loss or theft of the card[27]. This notification is equally important for banks, which can take immediate action to stop financial losses. Remembering which number(s) to call to report lost and stolen cards may be difficult if the customer owns more cards, is travelling abroad or is in a situation of distress. Therefore, a single telephone number for declaring lost and stolen payment cards in Europe would be of significant value to citizens.

On 15 February 2007, the Commission adopted a decision reserving the whole range of phone numbers beginning with "116"[28]. These numbers should be freephone numbers (e.g. the cost of the call should not be borne by the citizen) and should be only used for "harmonised services of social value" in accordance with the definition and conditions set out in the Commission Decision. Immediately after adoption of the Commission Decision, the Commission services launched a public consultation inviting interested parties to propose specific 6-digits numbers in the sub-range 1160XX and 1161XX to be reserved for specific services. An interested party introduced a request to consider card (or more generally payment instrument) stop services as services of social value and to consider reserving 116116 for these services. The decision to allocate a 116 number to card stop services has still not been

---

is on ATMs, the Group also focuses on all payment terminals that have a direct impact on crime perpetrated at ATM locations. See www.eas-team.eu.

25 In principle, by the end 2010 magnetic stripe-based transactions will no longer be SEPA Card Framework compliant.

26 Article 61(4) regarding liability indicates that "the payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with Article 56(1)(b), except where he has acted fraudulently. Article 61(5) further indicates that "if the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument as required by Article 57(1)(c), the payer shall not be liable for the financial consequences resulting from use of that payment instrument (except where he has acted fraudulently)".

27 Article 56(1)(b) requires the payment service user to notify the payment service provider (or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use. Article 57(1)(c) requires the payment service provider to ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 56(1)(b) [or to request unblocking pursuant to Article 55(4)].

28 Commission Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with '116' for harmonised numbers for harmonised services of social value, OJ L 49, 17.2.2007, p.30.

taken by the Commission pending, *inter alia*, the verification of the payment industry interest in using such a single freephone number in other Member States.

4.2. Non-face to face situations

4.2.1. Card-not-present fraud

The EMV success (see above) has resulted in an overall decrease of card fraud losses[29], but at the same time generated a de facto shift of payment card fraud towards remote (e.g. non-face to face) situations, mostly in the Internet environment: the so-called card-not-present fraud. This type of fraud is increasing in Europe[30] and is considered to constitute the highest threat for payment cards[31].

Card-not-present fraud consists in the misuse of illegally obtained card data in mail and telephone orders, but essentially in Internet payments (e-commerce[32]). The growth of this type of fraud has additionally given rise to the development of websites dedicated to the massive selling of illegally obtained[33] card data with a view to their fraudulent use[34].

Criminals have been taking advantage of gaps in the security requirements applied by the payment industry and e-commerce sites in relation to the acceptance of (credit) card transactions: not all merchants have systematically been collecting the card security codes (the numbers on the back of the card, also known as CVX2 numbers, which cannot be skimmed) while payment card issuers have not systematically rejected transactions with false or no card security code. The airlines/travel agencies and gaming/gambling sectors have been identified as weak areas.

In reply to this threat, the EPC recommends ensuring the use of the card security codes as from January 2008 (unless other fraud prevention methods leading to similar or better results can be applied). This wider use of the codes should lead, in the present circumstances, to a large diminution of fraud. Additionally, the payment industry is providing incentives to merchants and cardholders for the use of enhanced secure verification methods in internet payments (so called 3D Secure), which are voluntary at this stage. The payment industry has also engaged in recent times in specific dialogue with airlines on fraud issues, as this is the sector in which fraud is higher.

---

29 Cf. EPC, *Resolution: Preventing Card Fraud in the New SEPA Environment*, (March 2007). See also the presentations of the EPC Card Fraud Task Force at the FPEG meetings of 2006 and 2007.

30 See the presentations of the EPC Card Fraud Task Force at the FPEG meetings of 2006 and 2007.

31 See Europol, *Organised Crime Threat Assessment (OCTA)*, June 2007, p.17: "Neither will increased security solve all problems for debit and credit cards. In fact, even if EU fully migrates to chip, PIN and secure code, the card data could be used elsewhere, in a simpler manner, in the rest of the world. Furthermore, the main threat for "plastic" payments is no longer represented by counterfeit cards, but by card-not-present (CNP) payments, where credit card transactions are carried out on the phone or on the Internet."

32 Payment cards are still the most popular payment instrument for e-commerce payments.

33 By skimming, hacking false merchant sites, staff fraud or other method.

34 See generally Europol, *High Tech Crimes within the EU: old crimes new tools, new crimes new tools – Threat Assessment 2007 (public version)*, August 2007, p. 27 and seq.

4.2.2. E-banking fraud

E-banking fraud also takes place in a remote transaction environment. The main threat relates to account takeover fraud. Bank customer data is obtained through spoofing[35], phishing[36], pharming[37], trojans[38] (or other viruses and similar malware), hacking[39] of databases, staff fraud etc. Data illegally obtained is then used, for instance, to empty the account through credit transfers[40].

One way to address e-banking is to increase the level of security associated with customer authentication methods. Currently, banks tend to consider the security features of their e-banking systems as part of their commercial policy. Hence, contrary to the situation for payment cards, there are no minimum market standards, although there is a (slow) convergence of authentication methods (see also section 6.3)[41]. In this context, the European Payments Council, encouraged by the ECB, has recently undertaken a survey on security issues related to customer authentication (customer-to-business) with regard to direct debit and credit transfer schemes. The objective is to produce a threat assessment (excluding card schemes) with a view to agreeing (possibly in 2008) on some best practices to recommend to the banking industry[42].

4.2.3. Identity theft/fraud and generally cyber crime

Both card-not-present fraud and e-banking fraud are, *de facto*, variations of the wider identity theft/fraud phenomenon[43], where the non-face to face dimension is important and whose impact seems to be growing. In the 2004-2007 Action Plan, the Commission already highlighted this problem and stressed the need to strengthen business and consumer confidence regarding non-cash means of payment. At the same time, to the extent that payment fraud is increasingly committed using electronic communications networks, it is

---

35 In the context of network security, spoofing refers to a situation in which a person or programme successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage.

36 Phishing is an attack perpetrated through the mass e-mailing of a message designed to appear as if it originates from a legitimate source. The message contains some suitable pretext for fraud, such as a bank requesting that the recipient update his online banking account information. The message may contain a link to a counterfeit copy of the legitimate Web page of the targeted bank. As part of this web page, the phisher spoofs a form that asks the e-mail recipient to provide his proprietary data (i.e. bank account number, personal identification number (PIN), valid credit card number and expiration date).

37 Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic to that web site to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses- the "signposts" of the internet.

38 A malicious program that is disguised as legitimate software.

39 Hacking refers to electronically breaking into databases where financial or other personal data is copied. This data is subsequently fraudulently used.

40 See generally Europol, *High Tech Crimes within the EU: old crimes new tools, new crimes new tools – Threat Assessment 2007 (public version)*, August 2007, p. 27 and seq.

41 For a description of different types of authentication methods, see generally European Commission, *Study on user identification methods in card payments, e-payments and mobile payments* (November 2007), Work Package 1, pages 19 and seq. See work package 2 regarding the use of authentication methods and work package 5 for an overall summary.

42 This could lead to the update or the replacement of the ECBS (European Committee for Banking Standards) *Security Guidelines for e-banking: application of Basel risk management principles*, TR411 (version2), August 2004.

43 In this paper, no distinction will be made between identity theft and identity fraud.

becoming a category of the wider cyber crime problem. These issues will be examined in section 5.2 below.

4.3. Fraud detection tools and the processing of personal data

The activities of cardholders and card acceptors are permanently monitored in real time by fraud detection tools operated by card issuers with a view to detecting fraud (for instance abnormal transactions) and being able to react to it in a timely manner[44]. This data processing is considered essential by the payment industry in the fraud prevention context[45].

The recent Directive on Payment Services recognises that in order to facilitate effective fraud prevention across the Community, Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud[46].

At the same time, to the extent that the operation of those fraud detection tools implies the processing of personal data, these activities should be conducted in compliance with the strict safeguards set in European privacy legislation[47]. As a result, the desire by the payment industry to process data beyond the card issuer sphere (for instance at card scheme level in a SEPA wide area) in order to increase its effectiveness is not exempt from problems. The FPEG discussed the data sharing issue in a number of different meetings and a report on the limits to the sharing of personal data for fraud prevention purposes was prepared by the FPEG secretariat in December 2006.

The question of the sharing of fraud related data will inevitably arise in the context of the implementation of the payment services directive, and notably from the perspective of achieving a level playing field at SEPA level. It should be stressed that there are already innovative solutions in some Member States such as Italy, where the public authorities act as trusted third parties for the pooling of data in full respect of the national data protection law[48].

It should be noted that the question of data sharing beyond the individual bank is of lesser importance in the context of e-banking fraud, where there normally will be little need (if any) for the bank to share fraud related data with others.

---

44 Card issuers and acquirers also operate other types of databases which contain information on fraud that already took place: e.g. databases of terminated merchants or of fraudulent transactions.

45 The ECB seems to also implicitly support this kind of fraud detection tools. See ECB, *Oversight framework for card payment schemes – standards* (January 2008), pages 11.

46 Article 69 of the Directive on Payment Services.

47 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

48 For a description of the new Italian database, see the presentation at the FPEG meeting of June 2007 – available at the FPEG website.

5. PROSECUTING PAYMENT FRAUD

5.1. The need for effective penalties

The deterrent effect of criminal penalties for payment fraud offences should be the first key element of the fight against fraud. Since 2001, Council Framework Decision 2001/413/JHA[49] has required Member States to criminalise payment fraud and to establish effective, proportionate and dissuasive criminal penalties, including, at least in serious cases, penalties involving deprivation of liberty which can give rise to extradition. The Commission presented in April 2004 and February 2006 two reports on the measures taken by the Member States to comply with this Framework Decision[50]. Some stakeholders have the perception that the penalties applied in practice at national level in this field are generally too low to be dissuasive[51]. Europol signalled in 2005 that national criminal laws are extremely lenient vis-à-vis fraud, thus inviting organised crime to resort more and more to this profitable and relatively safe type of crime, fraud being considered the archetypal low-risk high-profit crime[52].

5.2. Police and judicial responses

The effective prosecution of criminals is the second key element of the fight against payment fraud. There are, however, practical difficulties for the law enforcement authorities to ensure a fast reaction against fraud.

First of all, criminal conduct in relation to payment fraud is becoming highly technical and sophisticated. As a result, obtaining enough evidence to prove the actual criminal conduct is not always easy. The 2004-2007 Action Plan suggested exploring whether dedicated police forces could better contribute to the fight against payment fraud. It appears in this regard that the current trend in national police forces is to create specialised units to deal with cyber crime, including payment fraud committed in this environment, which is the fastest developing type of fraud.

Additionally, in large scale payment fraud there are normally significant cross-border components, while law enforcement authorities are limited by traditional territorial constraints: card data is generally obtained in one country but employed in another. This cross-border dimension is further complicated by the fact that large scale payment fraud appears to be committed by transnational organised crime and/or specialised ethnic groups with substantial mobility across borders[53]. Europol provides assistance, including analytical work, to national police forces in this fight, focusing in particular on skimming and carding

---

49 Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, OJ L 149, 2.6.2001, p.1.

50 European Commission, 30.4.2004, *Report of the Commission based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment*, COM(2004) 346 final; and 20.2.2006, *Second report based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment*, COM(2006)65 final.

51 See FPEG reports on ATM and POS security and on Identity theft/fraud.

52 Europol, *2005 EU Organised Crime Report (Public Version)*, pages 7 and 32.

53 See for instance Europol, *2005 EU Organised Crime Report (Public Version)*, pages 5, 7, 30; *2004 EU Organised Crime Report (Open Version)*, pages 8 and seq.

projects[54]. Additionally, in order to enhance cross-border police and judicial cooperation and assistance, a Joint Investigations Team network supported by Europol and Eurojust was created in 2005[55]. There have already been encouraging results leading to the disbanding of specialised criminal gangs in payment fraud[56]. It should be noted, however, that the legal framework and developments at EU level regarding this issue are not payment fraud specific.

Stakeholders also believe that better enforcement of the procedures on freezing and recovery of proceeds from fraud is needed. This necessity has also been recognised at EU level several times, which has led to the recent adoption of legislative tools which should help in this process. The Council adopted in 2005 a Council Framework on confiscation of crime-related proceeds, instrumentalities and property[57]. The aim of this framework decision is to ensure that all Member States have effective rules governing the confiscation of proceeds from crime, *inter alia*, in relation to the onus of proof regarding the source of assets held by a person convicted of an offence related to organised crime. In 2007 the Commission published a report on the implementation of this framework decision[58]. Another Council Decision was adopted in December 2007 concerning the cooperation between Member States' Asset Recovery Offices in the field of tracing and identifying proceeds from, or other property related to, crime[59]. This decision enhances cooperation between the relevant national authorities involved in the tracing of illicit proceeds and other property that may become liable to confiscation by creating national Asset Recovery Offices and allowing them to communicate directly. Europol and Eurojust are cooperating with national authorities in this area[60]. On a wider geographical scale, a new Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on financing of terrorism was adopted on 3 May 2005[61]. This Convention, which specifically includes fraud as a predicate offence to money laundering, should enhance cross-border cooperation between EU countries and European non-EU countries in this field. The Commission submitted in September 2005 a proposal for a Council decision concerning the signature, on behalf of the European Community, of this Convention[62].

---

54 See Europol, *Annual Report (2006)*, p. 14. See also the cases reported in Europol Annual Reports in relation to the Liaison bureaux activities.

55 See Europol press release of 30 November 2007 ("Eurojust and Europol promoting joint investigation teams").

56 See for instance Europol press releases of 20 June 2007 ("Europol supports Italian *Carabinieri* in combating an international credit card fraud network") and of 15 March 2007 ("Successful co-operation and co-ordination activities have led to the dismantling of a credit card fraud network in Romania"). See also the cases reported in Europol Annual Reports in relation to the Liaison bureaux activities.

57 Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property, OJ L 68, 15.3.2005, p.49.

58 COM(2007)805 final, of 17.12.2007.

59 Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime; OJ L 332, 18.12.2007, p.103.

60 See Europol, *Financial and Property Crimes*, January 2006 p.1.

61 Convention n°198. The text of the Convention and the state of play of the ratifications is available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=2/6/2008&CL=ENG. This convention will replace the previous 1990 Convention (Convention n°141) on the same subject. Pursuant to the 1990 Convention, the Council adopted on 26 June 2001 a Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime; OJ L 182, 5.7.2001, p. 1. The Commission has prepared two reports on the implementation of this Decision: the first of 5 April 2004 (COM(2004)230final), the second of 21 February 2006 (COM(2006)72final.

62 COM(2005)426, of 13.09.2005. The formal Council decision has not yet been adopted.

5.3. Assisting tools

Europol continues to provide regular specialised training, in cooperation with payment card schemes, to national law enforcement authorities on operational aspects of payment card fraud, in particular on skimming and hi-tech payment card crime over the Internet. This specialised training improves the expertise and the financial investigation capacity of the law enforcement authorities in this field[63].

6. CHALLENGES AHEAD

6.1. Increasing the knowledge of the problem

Understanding the nature and the extent of the problem is of primary importance in order to evaluate the risks, implement the appropriate measures to counter fraud and measure their effectiveness. Referring to payment card fraud, Europol indicates that it is still an underestimated problem, especially its connections with other types of serious crime[64]. Nevertheless, the quality of statistics providing a picture of payment fraud at EU level could be largely improved, as should statistics on criminal justice in general.

Concerning payment cards, the EPC is developing an anti-fraud database that would integrate aggregated statistics on fraud covering both national and SEPA wide transactions[65]. This database is to be operated, in full respect of privacy protection rules, by a neutral trusted third party[66]. The database should normally be operational in 2008. A feasibility study and a prototype have been prepared by a group of European card schemes, with the support of the Community Programme AGIS[67].

Regarding e-banking fraud and notably phishing, victims, in particular financial institutions, are reluctant to report cases[68]. The risk of damaging the reputation of the firm is carefully considered by financial institutions before deciding to disclose the attacks. Other considerations play a role, *inter alia* the different approaches to the problem and different goals pursued by the financial institutions and by the police themselves. As a result, there is no reliable picture of the extent of the problem. It should be noted that in the case of phishing, financial institutions are by far the most targeted businesses by criminals. For Europol, this is one of the biggest constraints which impedes a real assessment of computer crimes.

In 2006 the Commission addressed the need to improve the statistics in the area of crimes and criminal prosecution by launching an ambitious 2006-2010 action plan on developing an EU strategy to measure crime and criminal justice [69]. The Action Plan aims at establishing a

---

63 See generally the annual reports of Europol.

64 Europol, *Annual report* (2006), p. 14.

65 EPC, *Resolution: Preventing Card Fraud in the New SEPA Environment*, (March 2007).

66 In reply to the Eurosystem's view of a "SEPA for Cards", the EPC suggests that the Eurosystem analyses the feasibility of acting as a trusted third-party for such data collection and its reporting. See, EPC, *A response to the Eurosystem's view of a "SEPA for Cards"*, 11 April 2007, Doc. EPC071/07.

67 See Annex 1 for further detail.

68 See Europol, *High Tech Crimes within the EU: old crimes new tools, new crimes new tools – Threat Assessment 2007 (public version)*, August 2007, p. 8-9. See also European Commission, *Study on user identification methods in card payments, e-payments and mobile payments* (November 2007), work package 5, page 39.

69 Communication from the Commission of 7 August 2006, *Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006-2010,* COM(2006)437.

methodology to develop EU statistics on crime and criminal justice that in the longer term will be comparable between Member States. The Commission will support the implementation of the Action Plan through the coordinated activities of an Expert Group (which will identify the needs for statistical data on crime and criminal justice) and of a European Statistical Office Expert Group (which will produce the necessary data)[70].

6.2. Fighting the new threats: payment fraud, identity theft/fraud and cyber crime

Payment fraud is a moving target. As mentioned in section 4.2, new threats appear, notably identity theft/fraud and, more generally, cyber crime (which includes many of the identity theft/fraud typologies). Community responses to these new threats have been numerous in recent years, either at regulatory level or by raising greater awareness. They are explained in more detail in the next subsections.

6.2.1. Payment fraud and identity theft/fraud

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. Identity data and supporting documents play an increasingly important role in financial and social processes and transactions, and therefore the data and the documents – rather than the persons themselves - increasingly become the subject of attack[71]. In some EU Member States identity theft/fraud is among the fastest growing type of financial fraud with increased involvement of organised crime. Furthermore, this kind of fraud has serious implications for its victims, which go beyond simple financial losses, to include emotional costs and the inconvenience for users of "cleaning up" their name.

As part of the awareness initiatives undertaken by the Commission services in the context of the 2004-2007 Action Plan, the Commission organised a High level Conference in November 2006 on identity theft and payment fraud[72]. The aim of the conference was to emphasize the importance of a wider involvement of policy makers and high ranking representatives of national administrations in this issue.

One of the main conclusions of the 2006 Conference was the need for a better understanding of the problem. A common definition of identity theft in the EU would be desirable (irrespective of the *modus operandi* and technical means used to compromise personal data),

---

70 The Commission also adopted in 2006 a Decision establishing an experts group on the policy needs for data on crime and criminal justice, with the possibility of creating specialised subgroups. Its main objective consists of assisting the Commission in identifying the needs for development of common indicators and tools designed to measure crime and criminal justice. This will also involve developing common indicators and other data needs specifically from the perspective of users of statistical data. See Commission Decision 2006/581/EC of 7 August 2006 setting up a group of experts on the policy needs for data on crime and criminal justice, OJ L 234, 29.8.2006, p.29.

71 See Europol, *Organised Crime Threat Assessment* (2007), p.17: "*In a world characterised by increasing anonymity and bureaucracy, documents are gaining more importance than the persons carrying them. Without a complete set of documents a living person does not officially exist, and at the same time a non-living, virtual person can cash money and social benefits by means of apparently genuine documents. Through them certain rights, entitlements and services are attributed to the bearer. Such a situation is and will be thoroughly exploited by organised crime. […] Identity fraudsters can steal the personal and financial data of an existing victim or fabricate a totally fictitious person with the aim of using debit and credit cards – sometimes after having opened a bank account – and spending money they do not have.*"

72 www.ec.europa.eu/justice_home/news/information_dossiers/conference_integrity/index_en.htm

as well as more statistical data in order to quantify the extent and the impact of identity theft. This should allow for a better tackling of identity theft at EU level, in particular by intensifying public-private cooperation and coordinating efforts to raise awareness. In this context, a similar high level conference was organised in November 2007 by the Portuguese presidency of the EU to examine the identity theft problem from a wider perspective. This conference reached similar conclusions[73]. Two follow-up activities to the 2007 conference were launched: (i) a glossary, to be built up, taking into due account the terminology already existing in reference studies and reports; and (ii) an analytical study on identity systems.

At the 2006 conference, support was also expressed for new EU penal legislation providing that the specific behaviours which concur to commit identity theft (including phishing and other forms of cybercrime) are criminal offences in all EU Member States. Following this, the Commission launched in 2007 an external comparative study on the legal instruments to combat organised crime related to identity theft in the EU Members States. Depending on the results of this study, expected for autumn 2008, the Commission may consider harmonising EU criminal legislation on identity theft in order to ensure that identity theft is a criminal offence in its own right in all EU Member States and to introduce effective dissuasive sanctions[74]. The need to strengthen investigations and prosecution through law enforcement was also emphasized at the conference.

Facilitating the reporting by victims of identity theft was also discussed at the conference[75]. Participants suggested the creation of an EU contact point where communications related to identity theft could be sent for possible follow up. Similarly, the 2004-2007 Action Plan suggested exploring the merits of establishing such a contact point. This examination is still pending.

Assisting the private sector in the verification of identity documents was also highlighted as a desirable objective. On this issue, an EU database disseminating information on security features of authentic identity and travel documents to the public recently entered into operation. It is the "Public Register of Authentic Identity and Travel Documents Online" (previously known as the FADO project). The PRADO database is hosted by the general secretariat of the Council[76].

The FPEG also discussed the implications of identity theft/fraud for payment services. This was ultimately reflected in an FPEG report disclosed in 2007 which provides an overview of the identity theft/fraud problems in the payment and retail banking areas, whilst recognising that the effects of identity theft/fraud go well beyond the financial sector. The report outlines the main risks and the vulnerabilities all along the identity chain in the financial system. This report highlighted in particular the importance of maintaining the integrity of the identity chain. Currently the weakest links of the chain are: the customer's computer, the Internet Service Providers, the data storage service providers acting as third parties, as well as the databases operated by merchants and public authorities. This report also highlighted that although technology is part of the solution, it is not the only solution. Better education of the

---

73 This conference was wider in scope and its conclusions covered a wider range of issues: www.idfraudconference-pt2007.org

74 See also the Communication from the Commission of 22.5.2007, *Towards a general policy on the fight against cyber crime*, COM(2007267final, p.10.

75 See section 5.1 above on the reluctance of financial institutions to report fraud cases because of the reputational implications.

76 www.consilium.europa.eu/prado/EN/homeIndex.html

weak parties (citizens, SMEs) in the use of the Internet, as well as providing care for the victims, are also necessary, in order to improve trust.

The identity theft/fraud problem has implications for the wider perspective of identity management. During the past years there have been a number of initiatives from industry, academia and international organisations to define user-centric identity management concepts, that minimise the scope for identity abuse and shift the balance to the user to make essential decisions about the use of his/her identity information. The Commission has funded research projects in this area through the 6th Framework Research Programme (FP6), notably the PRIME[77] and FIDIS[78] projects. It remains to be seen whether it is possible at this stage to develop standardised user-centric meta-level identity definitions. This could be the basis for a competitive market for identity providers, add customer empowerment and consumer choice, and open up a wide array of commercial opportunities that rely on trustworthy services.

Recently, as part of 7th Framework Research Programme (FP7, 2007-2013), a new set of information and communication technologies security projects[79] was launched. Many of these projects directly target data and privacy protective identity management (for example PRIMELIFE, PRISM, SWIFT, TAS3) or focus on specific authentication technologies, such as revocable biometrics (biometrics are increasingly used for authentication purposes and therefore could become a target for criminals, see for example the projects TURBINE, MOBIO). Other projects focus on advanced encryption technologies for protecting data or devices (ECRYPT II, TECOM), or target securing networks, including mobile networks that are increasingly used for financial transactions, and securing business and data policies (for example CONSEQUENCE, MASTER, AWISSENET, INTERSECTION).

In this context, the Commission is also sponsoring research on and promotion of the use of interoperable electronic identities (eID)[80]. A large scale pilot project, STORCK, is being considered to be funded in 2008, through the ICT-PSP programme, with almost 20 Member States in order to promote interoperability of eID for government services (with 10 Million € financed by the ICT-PSP of the Competitiveness and Innovation Framework Programme). The Commission is also working on interoperability issues by establishing a "European Interoperability Framework for pan-European eGovernment services" through the IDABC programme (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens)[81].

---

77 PRIME is a research project which aims at developing a working prototype of a privacy-enhancing Identity Management System. To foster market adoption, novel solutions for managing identities will be demonstrated in challenging real-world scenarios, e.g., from Internet Communication, Airline and Airport Passenger Processes, Location-Based Services and Collaborative e-Learning. The work on prototype development is a means to validate its new scientific and research results. See www.prime-project.eu.

78 FIDIS (Future of Identity in the Information Society) is a network of excellence supported by the European Community under the 6th Framework Programme for Research and Technological Development. See www.fidis.net.

Work Package 5 of the FIDIS project deals with identity theft. See in particular deliverable 5.1 (*A survey on legislation on ID theft in the EU and a number of other countries*, May 2005) and deliverable 5.2b (*ID-related crime: towards a common ground for interdisciplinary research*, May 2006.

79 www.cordis.europa.eu/fp7/ict/security/projects_en.html

80 See generally: www.ec.europa.eu/information_society/soccul/egov/index_en.htm and www.ec.europa.eu/information_society/activities/ict_psp/index_en.htm

81 www.ec.europa.eu/idabc

6.2.2. Payment fraud and cyber crime

Criminal activities are becoming increasingly sophisticated and internationalised, with greater involvement of organised crime. As stated in the latest Europol organised crime threat assessment, technology is a facilitator in various traditional crime types, including financial fraud. Furthermore, its abuse has also created altogether new forms of crime, in particular cross-border crime committed via the Internet[82]. Indeed, nowadays, the main target in high technology crimes is the violation of privacy and the theft of data[83], and the use of the Internet is the main vehicle for facilitating this criminal process[84]. Furthermore, it cannot be excluded that cyber crime is progressively becoming technologically more sophisticated (for instance by increasingly relying on malicious software capable of deviating on-line financial transactions etc.) rather than relying on social engineering techniques (such as phishing), which can be more efficiently tackled by improving consumer education[85].

In tackling security challenges for the information society, the European Community has developed a three-pronged approach. First, the EU institutions continue to develop policy with a view to improving network and information security, which continues to pose challenging problems. In 2005 the Council adopted a framework decision requesting Member States to criminalise certain attacks against information systems[86]. The Commission also presented in 2006 a specific communication on network and information security, identifying risks and possible work streams for the future[87]. The establishment of ENISA[88] in 2004 has also been a major step forward in the EU's efforts to respond to the challenges relating to network and information security.

Secondly, the regulatory framework for electronic communications includes security-related provisions. In particular, under the European privacy legislation[89], administrative authorities have the power to act against certain illegal practices related to payment fraud, notably: unlawful access to terminal equipment, either to store information – such as adware and

---

82 For example, spoofing, phishing and hacking are relatively independent crime types, the origin of which is traced back to the widespread use of information technology and the Internet. See Europol, *Organised Crime Threat Assessment (2007)*, p.18

83 This may be done in several ways, such as hacking, phreaking, cracking of passwords, phishing, identity theft, pharming, the spread of malicious codes etc.

84 See Europol, *High Tech Crimes within the EU: old crimes new tools, new crimes new tools – Threat Assessment 2007 (public version)*, August 2007, p. 4.

85 According to Europol (with reference to phishing, pharming, vishing and smishing), "one of the key points in combating social engineering is education: various studies have stated that in most cases, the incorrect behaviour of the user has made it easier for the perpetrator of the crime." See Europol, *High Tech Crimes within the EU: old crimes new tools, new crimes new tools – Threat Assessment 2007 (public version)*, August 2007, p. 31.

86 Framework decision 2005/222/JHA on attacks against information systems, OJ L 69, 16.3.2005, p.67. See in particular Articles 2 and 4 as well as recitals 3 and 4.

87 See generally Commission Communication of 31.5.2006, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment", COM(2006)251, in particular section 2.

88 ENISA was created by Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p.1. The main objective of ENISA is to develop expertise to stimulate cooperation between the public and private sector and to provide assistance to the Commission and Member States in the area of network security. See generally the work programmes of ENISA: www.enisa.europa.eu .

89 See generally the Commission Communication of 15.11.2006, *On fighting spam, spyware and malicious software*, COM(2006)688, in particular section 4.1.2.

spyware programs – or to access information stored on that equipment[90]; and misleading users into giving away sensitive information such as e-banking passwords or payment card details by phishing messages[91]. This regulatory framework for electronic communications is currently under review and in 2007 the Commission proposed modifications to three directives, including on security issues[92]. The Commission is, *inter alia*, proposing that consumers are informed if their personal data have been compromised as a result of a breach of network security.

A particular aspect of privacy relates to the prevention of database hacking, notably by promoting the use of privacy enhancing technologies[93]. The Commission organised a High Level Conference on public security, privacy and technology on 20 November 2007. The main part of the Conference focused on the deployment of privacy enhancing technologies into information and communication technologies, with a view to avoiding certain breaches of data protection rules that result in invasion of privacy (and on identity theft)[94]. This Conference followed a Commission Communication of May 2007 on promoting data protection by privacy enhancing technologies[95]. This Communication aims at involving a vast array of actors, including the Commission, national authorities, industry and consumers, to identify demands and technical requirements for these technologies, with a view to providing the foundation for user-empowering privacy protection services which reconcile legal and technical differences across Europe through public-private partnerships. The Commission also announced at the Conference that it would support the development of privacy enhancing technologies which are heavily dependent on the evolution of information and communication technologies, notably by providing financial support under the Fundamental Rights and

---

90 See Article 5(3) of the e-Privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p.37).

91 See Article 6(a) of the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.111.195, p.31).

92 The Commission presented a Communication on this issue in 2006 launching, at the same time, a public consultation on the future of the electronic communications regulatory framework. See Communication of the Commission of 29 June 2006, *On the review of the EU Regulatory Framework for electronic communications and services*, COM(2006)334, in particular section 5.5 dealing with network and information security. In November 2007, the Commission presented a report on the outcome of this review, with a proposal to modify three directives. See Communication from the Commission of 13.11.2007, *Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and Summary of the 2007 Reform Proposals*, COM(2007)696. See also the Commission proposal of 13.11.2007 for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services, COM(2007)697.

93 It should be noted in this context that Article 17 of the Data Protection Directive (Directive 95/46/EC) already lays down the data controller's obligation to implement appropriate technical and organisational measures and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive (cf. recital 46 and Article 14(3) of Directive 2002/58).

94 The presentations of the Conference are available at: www.ec.europa.eu/justice_home/news/events/news_events_en.htm
The Conference also addressed public security and technology issues.

95 Communication from the Commission of 2.5.2007, *on Promoting Data Protection by Privacy Enhancing Technologies (PETs),* COM(2007)228.

Citizenship Programme (for the period 2007–2013)[96]. The Commission will also conduct a study on the economic benefits of privacy enhancing technologies in order to be able to encourage enterprises to use them. The Commission will also encourage consumers to use privacy enhancing technologies through awareness raising campaigns.

Thirdly, there is already European legislation criminalising cyber fraud, notably payment fraud[97]. However, the threat of high technology crime is intensified by the fact that many of these new forms of high technology crime are difficult to detect and control by law enforcement[98]. Therefore, it becomes particularly important to involve all stakeholders in the fight against this phenomenon. In 2007 the Commission adopted a Communication[99] on cyber crime launching a general policy initiative to improve European and international coordination in the fight against cyber crime, with a particular focus on the law enforcement and criminal dimension. The objective of the Communication is to improve and facilitate coordination and cooperation between relevant authorities and experts in the EU; to develop, in coordination with Member States, relevant EU and international organisations and other stakeholders, a coherent EU policy framework on the fight against cyber crime; and to raise awareness of costs and dangers posed by cyber crime.

Regarding in particular the question of financial fraud, this Communication emphasizes, in its action points[100], the intention to promote the development of technical methods and procedures to fight fraud (and illegal trade) on the Internet, and also through public-private cooperation projects. It also announces that the Commission will continue and develop work in specific targeted areas, such as in the FPEG on the fight against fraud with non-cash means of payment in electronic networks. It is worth noting that the Communication also highlights the need to engage in dialogue with private operators, especially Internet service providers, with a view to blocking and closing down illegal Internet sites. This was also one of the conclusions of the 2006 Conference on identity theft (see above).

Finally, research in the area of technologies to make information systems more secure has played/is playing a role in the fight against payment fraud and cyber crime and identity theft/fraud in general. In the context of the Framework Research Programme(s)[101], the Commission has been supporting research projects in relation to information and communication technology security, notably in connection to electronic identity management[102], privacy protection, data loss prevention and underlying technologies such as encryption, trusted computing and revocable biometrics, network security and security in the

---

96 Council Decision 2007/252/JHA of 19 April 2007 establishing for the period 2007-2013 the specific programme Fundamental rights and citizenship as part of the General programme Fundamental Rights and Justice, OJ L 110, 27.4.2007, p. 33.

97 See notably Articles 3 and 4 of the Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, OL 149, 2.6.2001, p.1. See also Article 8 (Computer-related fraud) of the Council of Europe Convention on Cybercrime of 23 November 2001 (Convention No 185).

98 Europol, *2005 EU organised crime report (public version)*, p.34.

99 Communication from the Commission of 22.5.2007, *Towards a general policy on the fight against cyber crime*, COM(2007)267final.

100 *Op. cit*., p.10.

101 For further information on the Research Framework Programmes, see the Community Research & Development Information Service: www.cordis.europa.eu.

102 See above on FIDIS and PRIME.

Internet of the future. These are all technologies relevant to electronic financial transactions[103] (as well as to many other services) that critically depend on trustworthiness.

In addition, the EU has substantially increased the resources dedicated to security research and innovation. Further to the "Security and Safeguarding Liberties" programme (with a budget of approximately € 750 million for the period 2007-2013)[104], which is further described in Annex 1, the 7th Research Framework Programme (2007-2013) has, for the first time, a fully-fledged security research theme with a total budget of € 1,4 billion). The Commission presented in September 2007 a Communication on European Security Research and Innovation[105]. This Communication emphasises the importance of public-private dialogue in security research in order, *inter alia,* to fight organised crime. See annex 1 for further detail.

6.3. Maintaining user trust in payments

Fraud, even if it affects a minority of users, undermines the general confidence in payment systems. Hence, a key challenge of the work on the prevention of fraud should be to maintain user confidence in payments. This does not necessarily require new legislation (see above section 3 for the new legislative requirements, the development of SEPA standards and the oversight policy of the ECB) but rather the commitment of the parties involved to achieve this goal. In the light of the increasing cyber crime attacks and the development of cashless payments on line, this also requires trusting the information society in general.

6.3.1. Trust in payments

Strong authentication methods are needed for securing transactions, in particular to counter remote payment fraud, and thus to enhance trust in cashless payments. As foreseen in the 2004-2007 Action Plan, the Commission launched a study, completed in November 2007, which analyses, from the security and the user-friendliness point of view, the current and prospective cardholder verification methods on card payments, as well as user verification methods on e-payments and mobile payments[106]. The underlying goal of the study was to

---

103 See for instance, the ANTI-PHISH project (Anticipatory Learning for Reliable Phishing Prevention) is directly addressing a payment fraud problem. This project aims at developing improve anticipatory anti-phishing technologies that help to protect and secure the global email communication infrastructure. The scientific focus of the project is on trainable and adaptive filters that are not only able to identify variations of previous phishing messages, but are capable of anticipating new forms of phishing attacks. Such technology does not exist yet, but could greatly improve all existing methods used in spam and phishing filters. See generally www.antiphishresearch.org

104 Communication of 6 April 2005 from the Commission to the Council and the European Parliament Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, COM(2005)124.

105 Communication of 11 September 2007 from the Commission to the European Parliament and the Council on Public-Private Dialogue in Security Research and Innovation, COM(2007)511.

106 European Commission, *Study on user identification methods in card payments, e-payments and mobile payments* (November 2007). The study includes 5 work packages: 1) assessment of best and most used identification technologies from a security point of view, including payment industry barriers perception; 2) assessment of user friendliness of identification methods, including user barriers perception; 3) comparison of findings with previous study on user identification methods realised in 2003; 4) regulatory, contractual and commercial barriers assessment of best used identification technologies; and 5) recommendations. This study was conducted by external contractors, following a call for tenders. The study is available at the European Commission, DG Internal Market and Services website.

encourage the payment industry to provide the highest economically viable level of security for those electronic payments but with sufficient consideration of user-friendliness.

Nevertheless, concerning the security levels of authentication methods, the study shows (based on a survey conducted on consumers[107]) that trust in the use and user friendliness of those methods do not always go hand-in-hand, at least in the case of e-banking and e-commerce payments (e.g. non-face to face payments). Contrary to the situation for cards (where the PIN code is at the same time trusted and easy to use), in the case of online payments, there are trade-offs to be made: 1-factor authentication methods (such as static passwords) are considered to be more user friendly than 2-factor authentication methods. As stated in the latest Europol threat assessment[108], the perception is that the question of security features vs. user friendliness is clearly market-driven and is often solved by emphasising the latter to the detriment of the former. Although users are usually the weakest link in the chain, they are not necessarily given any choice on the security levels of the payment instrument.

Involving the user is therefore important to increase his/her confidence in cashless payment systems and to raise his/her awareness of security levels. Although consumers show a reasonable level of trust, the study shows that an important barrier against the use of cashless payments stems from the user's perceived lack of security (based on extraordinary negative experiences reported in the news)[109]. The study suggests introducing a more general legal obligation to communicate security-related information to consumers using certain electronic payment instruments as a means to reinforce user trust. This is to some extent achieved by the new Directive on Payment Services which, in its Articles 42(2) and 42(5) imposes certain information requirements on the use of the payment instrument and its personalised features. In the same vein, the ECB indicates that "*Issuers, acquirers, cardholders and card acceptors should have access to relevant information in order to evaluate financial risks affecting them"*

---

107 See work package 2 of the study.

108 Europol, *Organised Crime Threat Assessment* (2007), p.18: *"[Organised Crime] involvement in technology-facilitated crime or the use of technology as a facilitating factor, is largely dependent on the development of electronic forms of business, society and banking. As societies become more and more dependent on technology, OC will find new lucrative crime opportunities and exploit human weaknesses by attacking systems with insufficient security features. The question of security features vs. userfriendliness is clearly market-driven and is often solved by emphasising the latter to the detriment of the former. Nonetheless, the service- or device-user and the actual user behaviour still have to be considered the weakest link in the chain."*

109 The study identifies other barriers such as the high cost of some technologies. Interestingly, legal restrictions and obligations or contractual restrictions are not considered as important barriers against the development of cashless payments. The study provides seven main recommendations, addressed to all stakeholders, to overcome the barriers identified in the study. Concerning the recommendations of the study, it should be noted that the recently adopted Directive on payment services as well as the anti-money laundering directive (see above section 3.1) already address some of the concerns expressed in the study. Additionally, other recommendations are addressed generally to the stakeholders and that work is in progress regarding some of them (e.g. harmonisation of security evaluation in the context of SEPA, see above section 3.2).
See also OECD (2008), *Measuring security and trust in the online environment: a view using official data*, Working Party on Indicators for the Information Society, DSTI/ICCP/IIS(2007)4/final. According to the OECD survey, fears expressed by people who do not buy online are not fully justified by the problems experience by people who do buy on line. Lack of security of payments was a problem for less than 2% of online buyers. See in particular pages 26-34

[110].Interestingly, from the trust perspective, the study suggests that there is no need to reinforce the liability of the user.

At the same time, the user capacity should not be overestimated. In general, the consumer is the weakest link in security, in particular in the on-line environment, due to lack of knowledge and protection: consumers' PCs are not high-security devices. As well as assistance to victims, consumers need effective prevention and control systems. It is in their interest to make use of recommended security advice and of protection systems offered. Consumer associations in FPEG[111] meetings outlined the need to find ways to communicate on security issues. For them, consumers can only assume responsibility for risks that they can actually influence in terms of risk-avoidance and risk-minimization. There are indeed weaknesses in the systems that the consumer cannot really address. Solutions must be safe and but also convenient and understandable to be a success. Additionally, raising security levels in systems should be carefully made so as to avoid making the user become the victim[112]. In this context, the concept of trust is crucial and, according to consumers' views, it should rely on openness towards the consumer.

The importance of public awareness and education to enhance trust has been emphasised (in relation to identity theft and payment fraud), both by the FPEG and in the conclusions of the 2006 Conference (see above section 6.2). In this context, the Commission presented in December 2007 a Communication on consumer financial education. This communication sets out some suggestions to assist financial education providers in delivering high quality schemes and describes some planned initiatives to give practical assistance to those delivering financial education in the EU Member States. The communication indicates that, among other possible benefits to individuals, financial education can help people to avoid the pitfalls of payment fraud[113]. This communication followed a Commission Green Paper on retail financial services[114], where the importance of consumer confidence and the need to empower consumers were largely underlined.

---

110 ECB, *Oversight framework for card payment schemes – standards* (January 2008), p.10. See also the explanatory memorandum of the ECB standard, *op.cit*., p.10: *"[…] In a CPS this is especially true, since the operational risk, including fraud, could lead to financial losses for one or more of the parties involved. For example, lack of consistent and up-to date information on how to mitigate fraud – e.g. information on recognising skimming devices and protecting PINs – may cause financial loss and decrease confidence in the payment instrument. However the disclosure of sensitive information could endanger the security of the CPS.*
Relevant documentation for evaluating possible risks stemming from participation in the CPS should also be available to potential actors.
If issuers, acquirers, cardholders and card acceptors do not have access to information about the risks they face as a consequence of participating in a scheme, they may face potential risks stemming from clearing and settlement, and from fraud and/or chargeback obligations. […]"

111 See in particular the minutes of the June 2007 meeting in relation to identity theft and the minutes of the December 2007 meeting in relation to the presentation of the study on user identification methods.

112 See the first paragraph of section 6.2.1 on the risk of increased identity theft attacks as a way to breach security.

113 See, Communication from the European Commission of 18.12.2007, *Financial education*, COM(2007)808, in particular page 4. See also the opinion of FIN-USE (Expert Forum of Financial Services Users), *Financial Education: Changing to second gear – envisioning the way ahead*, (January 2008), in particular page 3.

114 See European Commission, Green Paper of on Retail Financial Services in the Single Market, 30.4.2007, COM(2007)226.

6.3.2. Trust in information society in general

The European Commission organised on 7 December 2007 a high-level seminar on end-users' trust in the information society[115]. Discussion focused on technology, dependence and perception, and trying to find the right approach to the security of information networks, including the question of identity management. One of the conclusions of the seminar was that the awareness and education of the user may be more important than technology. The technology exists (including privacy enhancing technologies), but the problems are in most cases due to human factors. While security should ideally not be an option, in practice it is, and it is difficult to oblige people to use more security. The Commission is preparing a Communication on information infrastructure protection[116].

7. CONCLUSIONS

The work conducted in 2004-2007 shows that while it is important to ensure the security of means of payment and payment systems, it is also important to improve consumer confidence and trust. The new legal framework for payments, including the "know your customer" obligations, as well as the development of SEPA by industry should provide a good basis for increasing both security and trust. Additionally, the measures adopted by the Commission, beyond the Action Plan, in relation to the prevention of and fight against identity theft/fraud and cyber crime, should also contribute to those goals.

In this context, increased consumer education and awareness as well as cooperation of all stakeholders involved appear key to a successful approach to the fraud problem. The Commission has been giving financial support to actions undertaken by stakeholders related to the prevention of/fight against fraud, notably in the context of the research framework programme(s) and of the Prevention of and fight against Crime programme. This support is likely to continue in the coming years (at least in the 2007-2013 period): information and Communication Technologies as well as Security are mentioned as objectives in the EU Seventh Research Framework Programme which will be operational during the period 2007-2013; the Prevention of and fight against Crime programme is also in place in that period.

---

115 www.ec.europa.eu/information_society/policy/nis/strategy/activities/awareness_seminar/index_en.htm

116 Communication from the Commission of 23.10.2007, *Commission Legislative and Work Programme 2008*, COM(2007)640, in particular page 26.

WEBSITE REFERENCES

Except where otherwise stated, documents cited in this report, are available at the following websites:

- Council of Europe

  www.coe.int

- ECBS (European Committee for Banking Standards)

  www.ecbs.org

- European Central Bank – Payments

  www.ecb.europa.eu/paym/html/index.en.html

- European Commission, DG Internal Market and Services – Prevention of payment fraud:

  www.ec.europa.eu/internal_market/payments/fraud/index_en.htm

- European Commission, DG Internal Market and Services – Payment services:

  www.ec.europa.eu/internal_market/payments/index_en.htm

- European Commission, DG Justice, Freedom and Security – Financing Programme

  www.ec.europa.eu/justice_home/funding/intro/funding_intro_en.htm

- European Commission, DG Information society – Network and Information Security

  www.ec.europa.eu/information_society/policy/nis/index_en.htm

- European Commission – Fraud Prevention Experts Group:

  www.ec.europa.eu/internal_market/fpeg/index_en.htm

- European legislation – Eur-lex:

  www.eur-lex.europa.eu

- European Payments Council

  www.europeanpaymentscouncil.eu

- Europol

  www.europol.europa.eu

ANNEX 1 - FINANCIAL SUPPORT TO THE PREVENTION OF AND FIGHT AGAINST FRAUD

(i) The AGIS programme until 2006

AGIS was a framework financing programme run by the Commission to help the police, the judiciary, professionals and representatives of victim assistance services from the EU Member States and candidate countries to co-operate in the fight against crime, by supporting the setting-up of Europe-wide networks, as well as the exchange of information and best practices. It also aimed at encouraging Member States to step up co-operation with applicant and third countries. AGIS ran from 2003 to 2006 and financed several projects in this field, following annual calls for proposals.

Some of the projects financed by AGIS were directly related to the prevention of and/or the fight against payment fraud:

- a training programme on 'certified payment card experts' for police officers, presented by police departments of 4 Member States. This project received in 2004 a grant of 66.329,77 EUR (59% of the project estimated cost);

- a cooperation network (Interbank Security Observatory) in relation to security of electronic payment services, presented by payment schemes of 3 Member States. This project received in 2004 a grant of 146.000,00 EUR (69% of the project estimated cost);

- a feasibility study for a pan-European card fraud information database, presented by a group of several European card schemes. This project received in 2006 a grant of 121.228,26 EUR (67,51% of the project estimated cost);

- a comparative study of the incidence and impact of the recruitment and/or infiltration by organised crime groups of persons employed within the retail banking sector, with the purpose of facilitating the commission of serious fraud, presented by a British university. This project received in 2006 a grant of € 317.660,00 EUR (69,91% of the project estimated cost);

Several other projects had an indirect relation to this subject, dealing with issues such as: protection of crime victims, cyber crime, high tech crime, theft and illegal use of electronic devices, joint investigation teams, judicial cooperation, cooperation on asset recovery etc.

(ii) The new programme on Prevention of and Fight against Crime, 2007 onwards

A new General financing programme for the period 2007-2013 on "Security and Safeguarding Liberties" was set up by the Council with a total envelope of 745 M€. This programme, managed by the Commission, represents a huge increase of EU financial intervention in the security area. It is divided into two specific programmes[117]: one on Prevention of and Fight against Crime (600 M€) and a programme on Prevention of Terrorism (140 M€). A separate programme deals with Criminal Justice (200 M€).

[117] See OJ L 58, 24.2.2007. .

The Programme on Prevention of and Fight against Crime[118] co-finances projects with a European dimension: either trans-national projects or national projects respecting certain conditions. It will also provide operating grants for NGOs. Its Annual Work Programmes 2007 and 2008 identified the prevention of financial crime as a priority objective.

The 2007 Call for Framework Partnership Agreements (which imply the need to work on a regular and stable basis with a network) was published in February 2007. The annual working programme for 2007 and the associated calls for proposals were published in May 2007. As a reserve list was created, action grants under the 2007 exercise are still being awarded by the Commission in 2008.

While full information on the selected projects is not yet publicly available, in 2007, a project presented by a grouping of consumer associations in relation to the protection of critical financial infrastructure was selected for funding. This project includes awareness raising activities and the creation of a website to collect information about cyber fraud in transnational payments. It strives at improving the cooperation between the public and private sector. It would result into the creation of a European technical catalogue of the fraud at the disposal of the judicial and police authorities on the basis of a net of alerts and information facilitated by entities and citizens.

The 2008 Annual Work Programme was published in December 2007. The 2008 Call for proposals for Framework Partnership Agreements and the Call for proposals for Operating Grants were published respectively in February and March 2008.

(iii) The Framework Research Programme

The Commission, both under the 6th and the 7th Framework Research Programmes[119], has been funding research actions in the area of information and communication technologies[120] with are directly or indirectly related to the prevention of and/or the fight against payment fraud. This was notably the case of the research in relation to identity management, with projects such as PRIME[121] or FIDIS[122].

Under the 7th Framework Research Programme launched in 2006, a research dimension on security has been added. The goal of the European Security Research is to make Europe more secure for its citizens while increasing its industrial competitiveness by: developing the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as, *inter alia*, acts of (organised) crime, while respecting fundamental rights including privacy; ensuring optimal and concerted use of available and evolving technologies to the benefit of civil European security; stimulating the co-operation of providers and users for civil security solutions; improving the competitiveness of the European security industry and delivering mission-oriented results to reduce security gaps.

---

118 Council Decision 2007/125/JHA of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime', OJ L 58, 24.2.2007, p. 7. See also www.ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

119 For the 7th Research Framework Programme (2007-2013), see: www.ec.europa.eu/research/fp7/.
For the 6th Research Framework Programme (2002-2006), see: www.ec.europa.eu/research/fp6/index_en.cfm + dates

120 www.ec.europa.eu/information_society/research/index_en.htm

121 www.prime-project.eu.

122 www.fidis.net

There is a convergence in the research actions under the Security theme and the Information and Communication Technologies theme, leading in particular to the launching in September 2007 of a joint call for proposals in relation to critical infrastructure protection (including banking and financial infrastructure). The aim is to protect critical infrastructures that can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, mismanagement, accidents, computer hacking, criminal activity and malicious behaviour and to safeguard them against incidents, malfunctions and failures.

ANNEX 2 - ACTION POINTS OF THE EU ACTION PLAN 2004-2007

	Action Points identified in the Action Plan	Implementation so far
1	The membership of the FPEG will be streamlined by identifying fraud prevention experts in each sector and/or country who will be responsible for acting as effective contact points within their countries and as multipliers of the work carried out in the Group.	The FPEG secretariat identified experts from the underrepresented sectors, notably consumers, who were invited to the meetings.
2	A steering group will be established within the FPEG in order to carry out more effectively the envisaged actions. The steering group will prepare the work of the FPEG and supervise the sub-groups' activities.	The steering group was created.
3	At least two meetings of the FPEG will take place each year.	One meeting was convened in 2005, two in 2006 and two in 2007
4	The FPEG will be responsible for the preparation of a communication plan addressed to EU citizens and professionals on the progress and effectiveness of the measures of the new Action Plan.	The FPEG and the Commission implemented several initiatives aimed at increasing awareness in relation to fraud prevention.
5	Two FPEG sub-groups on security issues and on user issues will be established. The subgroups will meet according to the timetable and topics indicated by the FPEG. New subgroups may be established by the FPEG.	Several subgroups were created: ATM security, communication, commerce, data management, identity theft, law enforcement issues and security evaluation,
6	Within the EU Fraud Prevention Expert Group, a Sub-Group on Security Issues will be established. The Sub-Group will include different stakeholders according to the topics covered.	A subgroup on security evaluation was created. .
7	The Commission will launch a study covering cardholder verification methods on card payments and user verification methods on e-payments and mobile payments.	The study was completed.
8	The Commission will, in co-operation with national data protection authorities in the Article 29 Working Party, clarify the limits and conditions for exchange of information related to fraud prevention. Alternatively, if adequate clarification cannot be achieved, the Commission will propose legislation to amend existing EU data protection rules.	A group on data management was created. Its secretariat prepared a report on the barriers to data processing, with the cooperation of the data protection authorities. The Payment Services Directive integrated a specific article in connection to the processing of personal data for fraud prevention purposes.
9	The Commission will expand the existing EU Fraud Prevention Webpage with information on initiatives by other organisations active in fraud prevention.	Specific webpages on the FPEG activity were created.
10	The Commission will organise, in cooperation with the payment industry, Europol and other stakeholders, pan-European training sessions for specialised law enforcement officers to grant them the status of certified experts, as well as update training sessions for already certified officers.	Some training initiatives have been organised by Europol and the international card schemes, and funded by the Commission.
11	The Commission will organise a second high-level conference for senior police officers, magistrates and prosecutors, to raise awareness on payment fraud and its impact on the financial systems. Consideration will be	A High Level Conference on identity theft and payment fraud took place in November 2006.

	given to organise such events periodically.	
12	The Commission will assess the possible benefits of establishing at national level specialised or dedicated units in fighting payment fraud.	Due to current trends in payment fraud, specialised units on cyber crime, encompassing the fight against payment fraud, tend to be created at national police level.
13	The Commission will promote the involvement of national competent authorities (created to fight against fraud and counterfeit in relation to the Euro bank notes) in the prevention of payment fraud.	Due to current trends in payment fraud, the synergies appear to be more closely related to the fight against cyber crime than to the fight against currency fraud and counterfeit.
14	The Commission will organise a seminar on fraud prevention for representatives of the private sector and public authorities of the new Member States.	A seminar for candidate countries was organised in March 2006.
15	Within the EU Fraud Prevention Expert Group, a Sub-Group on User Issues will be established. The Sub-Group will allow discussion at pan-European level within the retail sector and consumer associations and will include different stakeholders according to the topics covered.	Discussions on users' issues were integrated into the other subgroups, where appropriate.
16	The Commission will continue to discuss the implementation of a single phone number in the EU for the notification of lost and stolen cards.	The Commission has legally reserved in February 2007 the numbers beginning with 116 for services of social value. European card schemes may apply for the use of the same number across Europe for the notification of lost and stolen payment cards.
17	The payment card schemes should prepare common educational tools for merchants covering all types of cards.	No Commission action involved.
18	The Commission will assess the merits of establishing an EU single contact point for citizens and businesses on identity theft, which could include a register of bodies engaged in the prevention of identity theft.	The FPEG report on identity theft and the High level conference examined this issue.
19	The Commission will promote the creation of a database of original and counterfeit identity documents accessible to both public authorities and the private sector.	The PRADO database, disseminating information on security features of authentic identity and travel documents to the public, entered into operation in 2007. The PRADO database is hosted by the general secretariat of the Council
20	The Commission will organise, together with the payment industry, awareness raising initiatives on payment fraud for the authorities of the candidate countries for EU accession and other European countries.	A seminar for candidate countries was organised in March 2006.
21	The Commission will continue to cooperate with other countries, bilaterally and in multilateral fora such as the G8, in order to help combat and prevent fraud.	Fraud prevention was integrated in the bilateral and multilateral discussions with third countries in relation to the prevention of and fight against financial and economic crime.