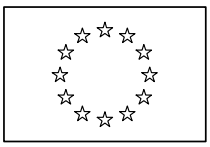

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20.10.2004
COM(2004) 679 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE EUROPEAN CENTRAL BANK AND EUROPOL

A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment

{SEC(2004) 1264}

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE EUROPEAN CENTRAL BANK AND EUROPOL

A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment

(Text with EEA relevance)

1. INTRODUCTION

In the EU Fraud Prevention Action Plan 2001-2003 (hereafter "FPAP")[1] the Commission undertook to submit after 2003 a report to the European Parliament and the Council on progress achieved in the implementation of the Plan and to propose, if necessary, additional or alternative measures. The Commission report on the FPAP[2] provides an assessment of the measures undertaken and their effectiveness. The present document complements the report and proposes future actions in this area.

2. BACKGROUND

In February 2001 the Commission adopted the FPAP in order to improve the prevention of fraud and counterfeiting of all non-cash payments. The FPAP aims at fostering a pan-European and coherent approach to fraud prevention. Single, isolated fraud prevention measures may be effective, but are not sufficient to tackle a threat such as payment fraud.

The specific reasons which led the Commission to issue an Action Plan were the following:

- The levels of fraud were relatively high. In 2000 the volume of fraud in the European Union was estimated at €600 million for payment cards only (approximately 0.07% of the payment card industry's turnover at that time).

- The rate of annual increase in fraud and counterfeiting was cause for concern. In 2000 fraud grew by approximately 50% in the EU. In particular, one of the areas where fraud increased the most was remote payments (made by phone, mail, or on the Internet).

- Proportionally to the volume of transactions, the scale of cross-border fraud was much higher than that of domestic fraud. However, at that time preventative measures were mainly taking place at national level.

- There was a growing involvement of organised crime. Criminal organisations demonstrated their ability to quickly change their *modus operandi* to circumvent countermeasures. Most important, the proceeds from fraud strengthen organised criminal groups. This is a stronger concern today, with the threat of terrorist financing.

---

1 Commission Communication "Preventing fraud and counterfeiting of non-cash means of payment", COM(2001) 11 final of 9.2.2001.

2 Working Document of the Commission Services no. … on a Report on the implementation of the EU Fraud Prevention Action Plan on non-cash means of payment.

- Fraud undermines consumer confidence in payment systems. For example, the risk of payment fraud is widely considered as one of the main barriers to the successful development of electronic commerce.

The key principle of the FPAP was cooperation among all stakeholders. Fraud prevention is principally the responsibility of the payment systems industry and the most important improvements are enhancements in the security of payments (such as the introduction of chip cards). However, all parties should be involved and play an active role in fraud prevention. Without a doubt, preventative measures are much more effective when implemented in partnership with all parties concerned. According to this principle, the FPAP was drafted in consultation with all stakeholders[3] and the Commission worked closely with these parties in implementing the various measures. The large majority of the actions foreseen in the FPAP were successfully completed[4].

3. TOWARD A NEW ACTION PLAN

It is widely recognised that the Commission's involvement in fraud prevention provided an added value. In the implementation of the FPAP, the Commission acted as a catalyst. It promoted a better information exchange, raised awareness and strengthened cross-border cooperation. In particular, it established a framework where fraud prevention specialists could meet and create synergies, including the exchange of best practices and educational material. As a result, the co-operation to prevent fraud has intensified, notably at cross-border level.

In the period covered by the FPAP, the combined initiatives of the payment industry, national authorities and other parties led to a reduction of the annual growth of fraud in the EU[5]. The FPAP also helped bring increased attention to the issue of payment fraud.

These initiatives must be continued in order to keep momentum. As always fraud is evolving. Criminal actions such as data hacking or identity theft[6] are growing at a worrying pace and new scams are emerging.

The Commission therefore intends to continue its action against payment fraud by issuing a new EU Fraud Prevention Action Plan covering the period 2004-2007. Most of its actions are the continuation or the follow-up of actions already undertaken. The new FPAP has been drafted in consultation with the EU Fraud Prevention Expert Group and other relevant groups[7]. It will complement the Directive on payment services in the Internal Market, which the Commission will propose in 2005, in underpinning the creation of a Single Payment Area

---

3 Such as payment card schemes, banks, national Ministries and Central Banks, law enforcement, the European Central Bank, Europol, Interpol, the retail sector, network operators and consumer associations.

4 For the details, see the Commission report on the implementation of the Action Plan 2001-2003, Working Document of the Commission Services no. … or http://europa.eu.int/comm/internal_market/payments/fraud/index_en.htm

5 In 2000 fraud was growing approximately 50% a year, much faster than today (15-20% a year).

6 Identity theft is the misuse of personal data to impersonate another individual without his or her consent. It usually includes the abuse of the victim's banking facilities.

7 Such as the Card Fraud Prevention Task Force of the European Payment Council. Input was provided also by individual Members of the Payment Systems Market Group and the Payment Systems Government Expert Group. Europol and law enforcement experts were also consulted.

in the EU. It should notably continue and further strengthen the existing initiatives to prevent fraud and contribute to maintain and increase confidence in payments.

Priority areas will continue to be the security of payment products and systems and increased co-operation between public authorities and the private sector. Clarification of existing EU data protection legislation with respect to fraud prevention activities is necessary to allow an effective and wider exchange of information, notably at cross-border level. The integration of new Member States in the EU fraud prevention framework and stronger relations with public authorities in third countries will continue to be a priority. Emerging threats will also be addressed.

4. THE EU FRAUD PREVENTION EXPERT GROUP

Objective:

⇒ The EU Fraud Prevention Expert Group (hereafter "FPEG") should be strengthened and its functioning should be re-organised.

In the FPAP the Commission set up the EU Fraud Prevention Expert Group (hereafter "FPEG"), which includes all major stakeholders in payment fraud prevention in the EU[8] and provides an added value as a platform where stakeholders could effectively exchange information and best practice to prevent fraud. It contributed to intensify cooperation between interested parties to prevent fraud, especially at cross-border level.

With the recent EU enlargement, gathering representatives from all interested sectors and of all Member States into one group while maintaining efficient working procedures becomes all the more challenging. A re-organisation of the membership and functioning of the group and an expansion of its mandate are necessary.

Action points:

⇒ The membership of the FPEG will be streamlined by identifying fraud prevention experts in each sector and/or country who will have the responsibility to act as effective contact points within their countries and multipliers of the work carried out in the Group.

⇒ 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 works of the FPEG and supervise the sub-groups activities.

⇒ At least two meetings of the FPEG will take place each year.

⇒ 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.

[8] The Group includes representatives of national and EU payment schemes, banks, national Ministries and Central Banks, law enforcement agencies (including Europol and Interpol), the European Central Bank, retailers, consumer groups and network operators.

⇒ Two FPEG sub-groups on security issues and on user issues will be established. The sub-groups will meet according to the timetable and topics indicated by the FPEG. New sub-groups may be established by the FPEG.

5. TECHNOLOGICAL DEVELOPMENTS

Objectives:

⇒ The payment industry should provide the highest economically viable level of security for electronic payments.

⇒ The manufacturers of payment products, the payment service providers and national authorities should implement a co-ordinated and structured approach to the security evaluation of payment products and components. The transparency of security evaluation procedures should be improved and standardisation should be promoted.

The migration to chip cards in the EU within a reasonable timeframe would increase security, help reduce fraud and boost user confidence. It is a priority which requires concerted efforts by all stakeholders. The Commission and national authorities should be prepared to assist the migration to chip cards in the EU, if necessary.

The payment industry is implementing new, more secure solutions for e-payments and mobile payments[9]. These efforts should be monitored and assisted.

In order to build confidence in payments it is essential for stakeholders to know the level of security of a payment product or component, both in absolute terms and with respect to similar products. At present security evaluation procedures are not based on common testing standards and there is little transparency toward the users. Banks and merchants could make better decisions if they knew to what extent one product is more secure than another. Users' confidence would increase if they received more detailed information about the testing carried out. Common security evaluation criteria and procedures could drastically reduce the costs and time of security evaluation, It is however essential that a harmonisation of security evaluation criteria does not reduce the existing level of security.

Action points:

⇒ 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.

⇒ The Commission will launch a study covering cardholder verification methods on card payments and user verification methods on e-payments and mobile payments.

[9] For example those based on the 3D Secure protocol.

6. EXCHANGE OF INFORMATION

Objective:

⇒ All stakeholders, while respecting the rights and freedoms of individuals and competition rules, should be able to exchange information for an early detection and notification of fraud attempts.

The activities undertaken in this area under the first FPAP should be continued. The main issue identified was the impossibility to exchange data on high-risk and fraudulent merchants within the EU. A clarification and harmonisation of the data protection rules in the EU with respect to fraud prevention activities is necessary to allow a wide cross-border exchange of information. Such clarification should balance the interests of fraud prevention with the respect of the fundamental rights of individuals. The EU Article 29 Working Party[10] established an informal sub-group of representatives of national data protection authorities and of the payment industry to discuss specific issues. In the response to the consultation document on a New Legal Framework for Payments in the Internal Market[11], strong support was expressed in favour of a full harmonisation of the EU data protection legislation on this subject. The works of the Article 29 Working Party Sub-group are still under way. Apart from the exchange of data on high-risk and fraudulent merchants, further activities where a clarification of the legislation is necessary should be identified. New initiatives (eg databases) could be considered in order to collect and exchange information more widely among fraud prevention specialists.

The EU Fraud Prevention Webpage[12] could be further developed into a pan-European reference point on the prevention of payment fraud in the EU available to citizens, businesses and governments.

Action points:

⇒ 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.

⇒ The Commission will expand the existing EU Fraud Prevention Webpage with information on initiatives by other organisations active in fraud prevention.

---

10 This Group, established under Article 29 of Directive 95/46/EC, includes representatives of the EU national data protection authorities. Its secretariat is held by the Commission (see http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm)

11 Commission Communication on a New Legal Framework for Payments in the Internal Market (COM(2003) 718 final).

12 http://europa.eu.int/comm/internal_market/payments/fraud/index_en.htm

7. TRAINING PROGRAMMES, EDUCATIONAL MATERIAL AND COOPERATION

Objectives:

⇒ The training of law enforcement authorities and the awareness of magistrates and public prosecutors on fraud prevention should be further strengthened.

⇒ The cooperation among EU administrative authorities to prevent payment fraud should be increased.

⇒ The ability to investigate fraud cases of national law enforcement should be improved.

The EU Card Fraud Forum held in 2003 offered a useful platform to share experience and ideas on payment fraud between the judiciary, law enforcement and the private sector. The awareness raising action with the judiciary and the initiatives to strengthen law enforcement training should continue, in view of a more effective investigation and prosecution of these crimes.

In law enforcement training a clear priority should be given to coordinated European training. It is also important that comprehensive training packages for law enforcement are prepared and updated, respecting the primary role and responsibility of national authorities and targeting on transnational aspects where European training presents a real value added.

In some Member States, specialised central units have been set up to better fight payment fraud[13]. The establishment of national specialised or dedicated units could strengthen the investigative capacity and facilitate co-operation with other law enforcement units and market participants.

The measures taken for the protection against currency counterfeiting may provide a useful indication on the action to be taken with regard to fraud prevention on non-cash means of payment. For the protection of the euro against counterfeiting a framework establishing the organisation and co-ordination of all public and private authorities was introduced. A Regulation lays down specific measures for the protection of the euro[14] and the Council assigned to the Commission the co-ordination of training and technical assistance, through a Decision establishing a specific financial programme[15]. The European Central Bank has established and maintains the CMS (Counterfeit Monitoring System) database on counterfeits and analyses new types of counterfeit banknotes. Europol is responsible for the transmission and analysis of information and established a database including criminal data for use by law enforcement. The Commission/OLAF monitors the implementation of legislation and prepares legislative initiatives, manages the "Pericles" training and technical assistance

---

13 For example the Central Office for the fight against crime linked to the use of information technology (OCLCTIC) in France or the Dedicated Cheque and Plastic Card Unit (DCPCU) in the United Kingdom.

14 Council Regulation (EC) N° 1338/2001 of 28 June 2001 laying down measures necessary for the protection of the euro against counterfeiting, OJ L 181 of 4.7.2001 p. 6

15 Council Decision of 17 December 2001 establishing an exchange, assistance and training programme for the protection of the euro against counterfeiting (the 'Pericles' programme), (2001/923/EC), OJ L 339 of 21.12.2001 p. 50.

programme and analyses new types of counterfeit euro coins. Member States have established National Central Offices for the protection against counterfeiting and designated bodies responsible for the technical analysis of counterfeits. They have also introduced legislation obliging credit institutions to withdraw from circulation and hand over counterfeits to competent authorities. Member States carry out training and technical assistance actions for the protection of the euro under the coordination of the Commission.

Accordingly, the competent national administrative authorities in the EU should be more involved also in the prevention of fraud on non-cash payments and their cooperation and coordination should be established. A framework for the training of administrative authorities with EU funds could also be considered.

As from 2004 the ten new Member States should fully participate in the EU initiatives. Notably, they will have to implement the EU penal legislation and integrate the framework of preventative measures which has been established.

Action points:

⇒ 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.

⇒ 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 given to organise such event periodically.

⇒ The Commission will assess the possible benefits of establishing at national level specialised or dedicated units in fighting payment fraud.

⇒ The Commission will promote the involvement of national competent authorities in the prevention of payment fraud.

⇒ The Commission will organise a seminar on fraud prevention for representatives of the private sector and public authorities of the new Member States.

8. OTHER FRAUD PREVENTION MEASURES

Objectives:

⇒ EU citizens should be provided with more and clearer information on the security of payments.

⇒ Merchants should benefit from the use of improved educational material and be provided with adequate tools to prevent data hacking.

⇒ The notification of lost and stolen cards in the EU should be improved.

⇒ Specific initiatives should be undertaken to prevent identity theft in the EU.

The exchange of information on existing educational material within the retail sector and consumers' associations is still limited, especially at cross-border level. Best practice remains to be achieved in guidelines to consumers on the possible risks related to the use of non-cash payments and how best to avoid them. A Commission study on the security of e-payments[16] demonstrated that consumers are not well informed on the security of the instruments they use. In addition to improvements in the security of e-payments, providing the "right" information to consumers on security is an essential requirement for users' confidence.

The Commission study on the security of e-payments also shows that the retail sector does not always implement the best technology available, mostly due to the cost of new equipment. Better efforts are however necessary to protect merchant web-sites from unauthorised access. Some recent major hacking incidents attest the need for further preventative actions against cybercrime. Security breaches at databases of e-commerce merchants, where access was gained to customers' payment card numbers, provide increased opportunities for payment fraud. A further consequence is the intangible damage to the merchant's reputation and to the consumer perception on the security of the Internet and the use of payment instruments in this environment. This strongly undermines consumer confidence in e-commerce. The problem is further compounded by the fact that many intrusions are not reported to the police[17]. The recently established European Network and Information Security Agency (ENISA)[18] aims at achieving closer European co-ordination in this area. It could assist payment providers and retailers in improving their protection against cybercrime.

The objective of creating a Single Payment Area in the EU calls for additional efforts to improve trust and confidence in payments and better prevent fraud. This objective of a single domestic market further increases the desirability of a single number in the EU for the notification of lost/stolen payment cards[19]. Today it is technically feasible to have single EU numbers[20].

The Commission organised in February 2004 a workshop on identity theft under the EU Forum for the Prevention of Organised Crime. The workshop showed how identity theft is a cross-sector problem affecting governments, businesses and citizens, which is growing rapidly in some sectors or countries[21] and is often linked to organised crime. Comprehensive preventative measures against identity theft are needed, as the verification of identities is extremely important for the integrity of society.

Action points:

⇒ 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 include different stakeholders according to the topics covered.

---

16 http://europa.eu.int/comm/internal_market/payments/fraud/index_en.htm#prevention-study

17 Recent statistics indicated that 80% of cybercrime incidents in the financial sector go unreported (IDC and Gartner, November 2002).

18 http://www.enisa.eu.int/index_en.htm

19 http://europa.eu.int/comm/internal_market/payments/fraud/cardstopeurope/index_en.htm. See also

20 At present ETNS (European Telephony Numbering Space) and UIFN (Universal International Freephone Numbers) numbers are available. Other numbers may become available in the near future.

21 Identity theft is growing very fast outside the EU (US, Canada, Australia) and is very relevant in the UK. For now, it is not equally prominent in the other EU Member States.

⇒ 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 payment card schemes should prepare common educational tools for merchants covering all types of cards.

⇒ 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 the prevention of identity theft.

⇒ The Commission will promote the creation of a database of original and counterfeit identity documents accessible to both public authorities and the private sector.

9. RELATIONS WITH THIRD COUNTRIES

Objective:

⇒ Third countries should introduce and enforce effectively preventive measures to combat fraud and counterfeiting of non-cash means of payment.

The dialogue with third countries should be strengthened in order to avoid that criminals operating from third countries might affect the interests of EU citizens and businesses. The Commission will take this forward both through multilateral groups, such as the G8, and through bilateral contacts.

Existing Accession Countries[22], and countries belonging to the Wider Europe[23] are areas of concern for fraud prevention. The progressive involvement of these countries in the EU fraud prevention policy calls for stronger relations with public authorities in these countries.

Action points:

⇒ 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.

⇒ 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.

10. FOLLOW-UP ACTIVITIES

After the end of 2007 the Commission will prepare a report to the European Parliament and the Council on progress achieved in the implementation of the Plan and will propose, if necessary, further measures.

[22] Bulgaria, Romania, Turkey, Croatia.

[23] For example Russia and Ukraine.