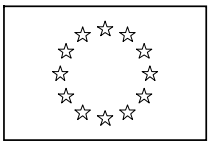

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 9.2.2001
COM(2001) 11 final

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

Preventing fraud and counterfeiting of non-cash means of payment

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

Preventing fraud and counterfeiting of non-cash means of payment

(Text with EEA relevance)

1. INTRODUCTION

This Communication builds on the 1998 Communication on fraud and counterfeiting of non-cash means of payment[1]. It is a priority measure under the Financial Services Action Plan[2] and outlines a number of preventive measures to combat fraud and counterfeiting in payment systems. These are set out in the annexed Fraud Prevention Action Plan. This Communication complements the Framework Decision proposed in this area[3] and the initiative undertaken for the protection of the Euro against counterfeiting[4]. It also addresses the concerns expressed by the European Council in Tampere and in Lisbon[5]. The Parliament has repeatedly underlined the importance of having the highest level of security for payment instruments[6] and invited the Commission to propose specific preventive measures. Efforts to combat fraud and counterfeiting are particularly important for the development of e-commerce.

2. NATURE AND EXTENT OF FRAUD

The level of cross-border fraud is higher than that of domestic fraud. In the top ten issuing countries of the European Union the rate of cross-border fraud for payment cards is several times higher than the overall EU fraud rate[7] and in some third countries, the cross-border fraud rate is even higher. However, prevention initiatives have been primarily taken at a domestic level. Fraud is increasing most in relation to remote payment transactions, especially on the Internet. And while sales in e-commerce in recent years have exceeded the most favourable estimates, its potential is inhibited by lack of confidence in the privacy and security of payment transactions performed over the Internet. Apart from the interception of data in payment transactions the possibility of hackers collecting information out of web-site data-bases is cause for concern.

Criminal activity has grown rapidly with the increase in the volume of payment transactions: the current proceeds from payment card fraud are estimated at €600 million in the Union[8], growing by approximately 50% last year. These profits may often subsidise other criminal activities and strengthen organised criminal groups. Fraud using stolen or counterfeit non-cash payment instruments is primarily carried out by criminal organisations. These are versatile in their operations (able to set up a factory to counterfeit payment cards in a matter of hours). They are also able to change their *modus operandi* to circumvent counter measures taken against them. Criminal groups often operate on a cross-border basis. Sophisticated techniques are used to commit payment fraud on the Internet.

3. THE CONTINUED IMPORTANCE OF PREVENTIVE MEASURES IN THE AREA OF TECHNICAL PAYMENT SECURITY

Efficient non-cash means of payment – which should be at the same time user-friendly, widely accepted, reliable and available at relatively low cost - are essential to a modern economy. Since efficiency is dependent on security, the introduction of the highest economically viable level of technical security is a prerequisite, and improvement of security levels should be measured by monitoring fraud statistics or by independent benchmarking of security.

In its 1998 Communication the Commission invited market participants to enhance the security of payment products and systems. The proposed Fraud Prevention Action Plan does not reiterate the need for new technology-based security features on payment instruments. Instead, it seeks to identify general objectives, to be achieved by promoting developments on technical security in general and the establishment of best practice.

The Commission has adopted a Communication "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime". This comprehensive policy statement covers criminal activity through the use of computer networks and services. It discusses the need and the possible forms of an initiative in the broader context of the Information Society, E-Commerce and Security objectives as described in the eEurope Action Plan[9] which includes focused actions, also on non-cash means of payment, to increase Internet security and achieve trust among businesses and consumers.

4. THE ACTION PLAN

Preventive measures to combat fraud and counterfeiting of non-cash means of payment are of fundamental importance. It is one of the fields of action suggested by the Commission in its global approach to crime prevention[10]. The Fraud Prevention Action Plan has at its heart close co-operation between the relevant public authorities and private parties, exchange of experience and information, training, development and sharing of educational material. Prevention is primarily a task of the payment systems industry (payment schemes, issuers, acquirers and manufacturers of payment instruments). The most important improvements are technical enhancements e.g. the introduction of chip cards. However, the Action Plan covers preventive measures that are most effective if implemented in partnership with all parties concerned e.g. holders of payment instruments, retailers and infrastructure network providers, national and international authorities, including law enforcement agencies. All parties should be aware of their role, responsibilities, rights and liabilities. It is also of key importance that consumers understand the risks of using non-cash payment instruments and the best preventive behaviour.

The Commission will co-ordinate action to enhance and promote preventive measures, including information gathering and awareness raising initiatives. It will also aim to attain a high level of fraud prevention through initiatives implemented evenly across the Member States of the European Union. These preventive measures shall be coherent with the initiatives taken in the global approach to crime prevention mentioned above.

5. CONCLUSION

The Commission invites the Council and the European Parliament to endorse the annexed Fraud Prevention Action Plan. It establishes a flexible approach. The Commission believes that isolated initiatives cannot offer optimal solutions. Fraud prevention can only be effective through a combination of co-ordinated preventive measures and a comprehensive regulatory environment,

including adequate sanctions. The Action Plan is based on partnership and co-operation at all levels. It will be reviewed periodically, the first review being no later than 2003. To this effect, by the end of 2003, the Commission will issue a report, which will assess the progress made in the implementation of the Fraud Prevention Action Plan and propose, if necessary, additional or alternative measures.

ANNEX

FRAUD PREVENTION ACTION PLAN

1. TECHNOLOGICAL DEVELOPMENTS

Objectives:

⇒ The payment industry should provide the highest economically viable level of security for remote electronic payments by mid 2002 at the latest.

⇒ All interested parties, especially national authorities, should contribute to implement a co-ordinated and structured security approach.

The payment industry has developed and implemented a wide range of technical fraud prevention measures. It is currently developing new technologies and implementing a comprehensive security strategy for both face-to-face and remote payments (e.g. introduction of the chip in credit cards[11] and new payment solutions for e-commerce).

The longer term objective is a co-ordinated and structured security approach by all interested parties (including national authorities). It is essential to promote the use of, and raise awareness on, standardised security requirements, which facilitate an objective evaluation of the security level of payment product or system. An example of such an approach are the Common Criteria/ Protection Profiles (now ISO standard IS 15408), which allow to define security requirements for information technology products and systems, including payment products. The implementation of such an approach could significantly enhance consumers' and merchants' confidence in payment products. The assessment of the highest economically viable level of technical security needs to be considered comprehensively, taking into account the total cost to all parties involved in payment systems.

Action points:

⇒ The Commission will organise awareness-raising initiatives, including a Forum on security of payment product and systems with regard to fraud prevention.

⇒ The Commission will launch a study on specific aspects of security of payment products and systems and their impact on fraud levels and in light of the outcome envisage specific initiatives.

2. EXCHANGE OF INFORMATION

Objective:

⇒ The payment industry and the retail sector, while respecting the rights and freedoms of individuals and the competition rules, should expand exchanges of information to promote an earlier detection and notification of fraud attempts.

Exchange of information is an essential element in any effective fraud prevention strategy; indeed, prosecution of payment fraud cases presupposes such an exchange between banks and law enforcement agencies both within and between EU Member States. The efficient information

exchange which exists within the payment industry and the retail sector for preventive purposes[12] in some Member States should be implemented more widely.

The implementation of the Directive 95/46/EC on data protection[13] poses conditions for the collection and exchange of information between operators in the payment markets and the authorities involved. The uneven implementation of that Directive[14] in the Member States may create problems for systems which rely on data to be collected in, and exchanged with, other Member States.

It is essential to have clear and common rules on the exchange of information taking place within each country and among EU Member States. This problem is relevant in an international perspective as well. The Commission will examine the extent to which the uneven implementation of the Directive has an impact on the fight against fraud and counterfeiting.

Action points:

⇒ The Commission will in co-operation with national data protection authorities, provide guidelines on limits and conditions for exchange of information related to fraud prevention.

⇒ The Commission will launch a "fraud prevention web-page" with information on initiatives related to fraud prevention and links to other relevant organisations.

3. TRAINING PROGRAMMES, EDUCATIONAL MATERIAL AND COOPERATION

Objectives:

⇒ The payment systems industry should implement in all EU Member States a comprehensive law enforcement training programme on preventing fraud and counterfeiting of non-cash means of payment.

⇒ Relevant players (including Europol and Interpol) should have access to information on training programmes and educational material for law enforcement.

Law enforcement training should be strengthened. It should cover cross-border aspects of fraud and remote electronic payment fraud, and possibly on the limits of the exchange of information in respect with data protection provisions; be complemented by comprehensive educational material and training tools specifically designed for police officers (including self-learning tools such as interactive CD ROMs); and be reviewed and updated to include the latest technological developments and the trends in international payment fraud. National authorities should consider law enforcement training as an essential tool for the effective investigation of payment fraud and allocate adequate human and financial resources for such training.

Investigating and prosecuting payment fraud cases should become a priority issue for law enforcement agencies, as the proceeds of these crimes may be used to fund other criminal activities. Awareness raising initiatives aimed at high-level national authorities are needed. Effective prosecution of payment fraud cases also requires the adoption of best practice in payment fraud investigations, the training of public prosecutors and magistrates and a framework of judicial co-operation among the Member States. The public authorities concerned should foster such initiatives. Initiatives to improve the quality and the presentation of evidence to law enforcement authorities would also facilitate cross-border co-operation between payment industry and law enforcement.

In addition, a mechanism to establish permanent dialogue between all interested parties (payment card schemes, banks, national payment schemes, Banking Associations, manufacturers of equipment and of payment cards, Europol, Interpol, public authorities, including law enforcement agencies, retail sector, consumers, network operators) would be useful in order to implement the proposed partnership approach and ensure maximum effectiveness in the fight against payment fraud and counterfeiting. This mechanism would also provide a useful contribution to the activities developed in the framework of the EU Forum on crime prevention.

Action points:

⇒ The Commission will organise a high-level conference for senior police officers, magistrates and prosecutors, to raise awareness on payment fraud and its impact on the financial systems.

⇒ The Commission will convene a meeting to encourage representatives of the payment industry and law enforcement, to identify key items of evidence needed to effectively investigate and prosecute payment fraud cases and to provide the information in an agreed format for cross-border information exchange purposes.

⇒ The Commission will organise expert meetings, representing all parties, to discuss issues related to fraud prevention, review the action points of the Communication and identify possible further preventive measures.

4. OTHER FRAUD PREVENTION MEASURES

Objective:

⇒ Parties involved should play their role in preventing fraud and counterfeiting of non-cash means of payment, and cooperate with each other.

The payment industry should in particular review the practices aimed at delivering payment instruments and the enabling devices (PIN or other code) to customers, to prevent to the utmost the exploitation of possible weaknesses in the payment system.

Fraud prevention experience must be shared between merchants and consumers in the Member States. The educational material qualified as "best practice" should be of high quality, be widely distributed in all Member States and be updated regularly. As educational material needs to be adapted to local needs, the contributions of retailers' organisations and consumers' associations is of paramount importance.

Consumers and their representative organisations should be actively involved in fraud prevention. Consumers' associations should raise awareness of the possible risks of fraud when using payment instruments, and should make suggestions on practical measures.

To avoid substantial losses from payment fraud[15], the latest technology should be made available to merchants. Retailers should protect their web-sites from unauthorised access and use of data. The retail sector should have updated information on the status of the payment instruments presented for acceptance and receive clear guidance on how to deal with suspicious transactions, especially at point-of-sale staff.

Mechanisms for prompt notification of loss or theft of payment instruments should be available, possibly entailing the introduction of a single, easily-remembered, toll-free number at EU level.

Consumers should not bear the consequences of payment fraud and be debited for transactions they did not perform. An equitable apportionment of liabilities between banks and consumers based on the provisions of the Commission's Recommendation 97/489/EC[16] should be introduced.

Electronic communications operators, that are actively involved in electronic payments, will play an increasingly important role in payments in connection with electronic money and mobile phone payments. They are invited to promote the use of appropriate techniques and assist the other parties.

National authorities and governments should regard payment fraud as a serious offence and accord priority to the prevention of fraud and counterfeiting. Fraud prevention measures should be evaluated and taken into account when new legislation in the financial sector is drawn up. Public authorities could oversee the evaluation on payment instruments performed by certification bodies authorities and bodies, since these need to be trusted by users. To introduce effective legal protection of non-cash means of payment in the European Union by 1.1.2002, date of introduction of banknotes and coins in euro, a speedy implementation of the Framework Decision on combating fraud and counterfeiting of non-cash means of payment, once it has been adopted, is needed.

Action points:

⇒ The payment systems industry should review its practices and procedures on an ongoing basis and discontinue or change those that may favour fraudulent behaviour[17].

⇒ The payment industry should establish best practice in educational material for retailers and consumers and produce new material as needed.

⇒ Retailers' organisations and consumers' associations should exchange information on educational material and identify the need for further, or improved, material. Consumers' associations should prepare guidelines on new risk areas (e.g. on-line payments) and fraudulent behaviour, and encourage consumers to take all reasonable steps to prevent fraud.

⇒ The retail sector should implement the most advanced technology which is economically viable. Retailers should be better informed on the status of the payment instruments presented for acceptance and advised on how to deal with suspicious transactions.

⇒ Consumers should benefit from a single phone line at EU level to facilitate their notification of the loss or theft of a payment instrument, or at least a single phone number for all issuers based in each Member State.

⇒ The Commission will organise a meeting with consumers' organisations and other interested parties to examine ways to develop and promote consumer education on the risks associated with different payment mechanisms and how best to avoid them.

⇒ The Commission will organise a meeting with a fraud prevention experts group representing all interested parties to examine the legal and economic guarantees and obligations of the different parties linked to fraud and counterfeiting of non-cash payments.

⇒ Governments and the national authorities should make efforts to improve trust and confidence in payment products. They should consider implementing expediently the proposed Framework Decision on fraud and counterfeiting of non-cash means of payment.

⇒ In 2003 the Commission will issue a report, which will review progress in implementing the Fraud Prevention Action Plan and propose additional or alternative measures

5. 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.

Co-operation with authorities of third countries is also essential to prevent fraud. While effective mechanisms are introduced in the European Union, measures should be taken to help prevent criminals affecting the interests of the European Union by relocating their activities to other countries.

The Commission will take this forward both through multilateral groups, such as the OECD, and through bilateral contacts. Greater information sharing and enforcement cooperation can help to identify emerging scams and threats to safe commercial transactions.

Action point:

⇒ The European Commission will organise, together with the payment systems industry, a seminar for the authorities of the candidate countries for EU accession, in order to raise awareness on payment fraud in these countries.

⇒ The Commission will cooperate with other countries, both bilaterally and through multilateral fora such as the OECD, in order to help combat and prevent fraud.

END NOTES

[1] Communication from the Commission to the European Parliament, the Council, the European Central Bank and the Economic and Social Committee: "A Framework for action on combating fraud and counterfeiting on non-cash means of payment", COM(1998) 395 final.

[2] "Financial Services: Implementing the framework for financial markets: Action Plan", COM (1999)232 of 11.5.1999.

[3] Proposal for a Council Framework Decision on combating fraud and counterfeiting on non-cash means of payment, COM(1999) 438 final of 14.9.1999.

[4] Proposal for a Council Regulation on the protection of the euro against counterfeiting, COM(2000) 492 final of 26.7.2000.

[5] The European Council in Tampere (October 1999) reaffirmed the Member States' commitment to reinforcing the fight against organised financial crime and specifically underlined the importance of preventive action, co-operation and the exchange of best practice. At the Lisbon Summit (March 2000) the European Council called on the Commission to consider how to promote consumer confidence in electronic commerce.

[6] The European Parliament adopted in November 1998 a Report and a Resolution on fraud prevention (A4-0396/98). The Parliament's Report sent a political message requesting strong commitment from the Commission and the Member States in the fight against organised crime.

[7] For these countries the cross-border fraud rate is equal to 0.40% of the international net sales volume, against a fraud rate of 0.07% for the total (domestic and cross-border) net sales volume (Source: VISA).

[8] This roughly corresponds to 0.07% of the payment cards turnover in the European Union.

[9] http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm

[10] Communication from the Commission "The prevention of crime in the European Union: Reflection on common guidelines and proposals for Community financial support", COM(2000) 786 final of 29.11.2000.

[11] To be completed by 2005 in the European Union according to the current plans (source: VISA and Europay/Mastercard).

[12] On-line "flagging systems" (for example CIFAS, which operates in the UK since 1988) allow the exchange of information on incidents of actual and attempted fraud between financial institutions and have been successful in reducing fraud. The payment industry has developed several databases on fraud analysis and risk assessment. Similar initiatives are taken in the retail sector, where incidents databases have been created.

[13] Directive 95/46/EC provides that personal information should be collected fairly and lawfully, for specific purposes and with adequate notice to the individual concerned. Data should be accurate, used only for the purposes declared when collected and should not be kept for longer than necessary to fulfil the stated purposes. The Directive gives the individual concerned, *inter alia*, the right to access the data, rectify it and object to its collection under certain circumstances.

[14] Member States have the possibility to derogate from the requirements of the Directive, if necessary, in order to prevent, investigate, detect, and prosecute criminal offences. However, as not all Member States may implement (or have implemented) this derogation, or have implemented it with the same scope, the collection and further processing of certain information mentioned above may be allowed in one Member State and prohibited in others.

[15] In particular regards the phone/mail order business and in e-commerce.

[16] Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder (OJ no. L 208, p. 52).

[17] For example, data which allow criminals to make fraudulent remote payment transactions with a credit card they do not possess, should be deleted, or disguised, from the sales vouchers.