COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 01.07.1998
COM(1998) 395 final

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 COMBATTING FRAUD AND COUNTERFEITING OF NON-CASH MEANS OF PAYMENT

Introduction

While the potential for economic growth in the Union is unprecedented thanks to the advent of the Single Market and to the Information Society, organised crime is however increasingly becoming a threat to society, organising itself across national borders and taking advantage of the free movement of goods, capital, services and persons. Technological innovations such as Internet and electronic financial services turn out not only to facilitate legitimate business, but also to be convenient vehicles either for committing crimes or for transferring the resulting profits into seemingly licit activities.

To ensure the orderly conduct of economic and social activity to the benefit of users and providers of goods and services, society requires sound, user-friendly, efficient, and secure payment mechanisms. A key to promoting the necessary confidence is to see to it that adequate guarantees exist that payment instruments may not be used for or in association with illicit activities.

The European Council in Dublin, December 1996, underlined its absolute determination to fight organised crime and stressed the need for a coherent and coordinated approach by the Union. Turning this resolve into concrete action, the European Council in Amsterdam, June 1997, endorsed an Action Plan to combat Organised Crime[1], in which, among other things, it calls on the Council and the Commission to examine and address, by the end of 1998, the issue of fraud and counterfeiting relating to all non-cash payment instruments, including electronic payment instruments.[2] This Communication focuses on non-cash payment instruments. The Commission is separately addressing the issue of falsification and counterfeiting of bank notes and coins in euro.

Purely national frauds are becoming international frauds. Payment card crime, for instance can be committed anywhere cards are accepted as a means of payment or for money withdrawal. As non-cash means of payment can be, as a rule accepted in non face-to-face transactions, they play a significant role in cross-border transactions, be they under traditional forms or in electronic commerce. Furthermore, large-scale frauds involve a multiplicity of "specialist" players and are mostly committed by organised groups of criminals. The sophistication and internationalisation of criminal behaviour demonstrate the need for a co-ordinated action at European level.

The need to address the problem of criminal activities directed at or involving payment instruments is gathering further momentum in the light of current and prospective institutional, economic and technological changes, notably:

---

1 Action Plan to Combat Organised Crime, adopted by the Council on 28 April 1997, OJ C 251, 97/C 251/01, 15 August 1997.

2 The Commission is presently preparing a Green Paper on the fight against counterfeiting and piracy in the Internal Market, which aims to protect intellectual property rights whilst allowing the proper functioning of Internal Market.

- the changeover to the Single Currency which, in particular throughout the transitional period before introduction of euro bank notes and coins, will be facilitated by the availability of transparent and secure electronic payment mechanisms;

- the advent of the Information Society and Electronic Commerce which, as is highlighted in the Communication on "A European Initiative in Electronic Commerce"[3], require efficient payment facilities.

A Commission study of 1997 on the forms of fraud occurring in the European Union, underlined in particular the frequency and considerable amounts involved in payment card fraud.[4] In December 1996 a conference was funded by the Commission, dealing exclusively with Organised Payment Card Crime, which further underlined these tendencies as well as the gaps existing in national legislation.[5]

1. The present Communication sets out the Commission's assessment of the problem, and proposes a framework of measures to promote an adequate *"security environment"* for payment instruments and the underlying systems. It consists of two components:

2. Firstly, the Commission presents (in Annex 1) a proposal for a draft Joint Action. The aim of the Joint Action is to ensure that fraud and counterfeit of non-cash means of payment is recognised as a criminal offence in all Member States, punishable by effective, proportionate and dissuasive penalties.

3. Secondly, a further set of actions is presented (in Annex 2) for consideration by all interested parties. In order to assess clearly what additional measures might be needed in this field, the Commission invites all interested parties to comment (in writing) to these actions no later than 31 December 1998 to:

The Director-General - DG XV
European Commission
Rue de la Loi 200
B-1049 Brussels
Fax: (+32 2) 295.65.00
E-mail: JOHN.MOGG@DG15.CEC.BE

---

[3] Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(97) 157 of 15 April 1997.

[4] The report from the study - *Fraud Without Frontiers* - is published at http://www.deloitte.ca/Whatsnew/Headlines/InternatFraud.htm

[5] The Final report of the project Co-operation to Combat Organised Payment Card Crime, organised by the Metropolitan Police, England, and the National Police Agency, The Netherlands, describes the research done as well as the results of the conference.

1. The nature and extent of the problem

Although non-cash means of payment includes an ever changing set of component systems or instruments (see section 2.a below) the main statistical evidence about the size of the problem of fraud and counterfeit is derived from the more senior systems, such as cheques and payment cards. The global payment cards industry turnover is fast approaching US $ 2.000 billion per year, out of which approximately US $ 3 billion is declared lost each year as a result from card crime. This may represent only 0,15% of volume, but still considerable amounts are affected, and in light of the expected growth in issuing of new cards by up to 25 % annually, the amounts are far from negligible. Approximately 25 % of all payment card losses are incurred by issuers in the European Union. Although losses have traditionally for the most part occurred domestically, increasingly they are incurred by card crimes originating abroad.

Measures to combat fraud are mainly taken domestically, which in several cases has led to at least temporary declines in the occurrences of domestic fraud, while crime shows its adaptability by increasing proportionally internationally. In addition to the problem of fraud and counterfeit associated with cheques and payment cards, a potential risk is that of the systemic fraud, i.e. attacks ("hacking") against the underlying computer networks which may also impact on the payment instruments and systems. Cross-border card crime is therefore a real issue for the Member States of the European Union as well as for the payment system industry and for users.

The European Parliament, consulted on a draft joint action aimed at the exchange of information between the law enforcement agencies and the payment card industry, insisted on the need for consistent and comprehensive action when adopting its resolution on 15 May 1998.

Payment services are not provided in a legal vacuum. The aim of the existing Community regulatory framework is the creation of a common single area, within which capital, people, goods and services may freely circulate. A brief summary of the constituting elements of such a framework is provided for in Annex 1.

2. The payment systems and their actors

This section describes non-cash payment instruments and underlying payment systems – their features - the main participants therein and their respective functions. Given the rapid development of the sector, the table below is purely indicative. Furthermore, the most innovative payment instruments may provide holders with the possibility of performing multiple functions.

a) Classification of payment instruments and systems according to their functions

For ease of analysis, payment instruments, with the exception of legal tender (i.e. bank notes and, to a large extent, coins), may include the following :

- *pre-paid paper* instruments (e.g. travellers' cheques, vouchers, bonuses, etc.)

- *stored-value electronic* instruments (i.e. pre-paid cards and software-based electronic money).
- traditional *paper* instruments (e.g. cheques),
- *traditional (quasi-)electronic* instruments (e.g. all types of payment cards, except for pre-paid cards: credit, debit, deferred debit cards, T&E cards) as well as
- *remote electronic banking* applications (i.e. home/phone/PC techniques).

PAYMENT INSTRUMENTS
(other than cash)

A1. Pre-paid paper Instruments	A2. Stored-value electronic Instruments
i) travellers' cheques	i) pre-paid cards
ii) vouchers	ii) software-based electronic money
Iii) bonuses	

B1. Traditional paper Instruments	B2. (quasi-) Electronic Instruments	B3. Remote electronic banking
i) cheques, bills of exchange	i) all types of payment cards (except pre-paid cards)	i) home/phone/ PC techniques
ii) paper and electronic credit/debit transfer orders	ii) paper and electronic credit/debit transfer orders	ii) paper and electronic credit/debit transfer orders

b) Definition of the actors in a payment system

Presently, under a payment scheme, the following recurrent participants (and functions) may almost invariably be identified:

- *"the issuer"*: this is typically the (financial) institution which, in the course of its business (pursuant to a contract concluded with the user) makes available to a user an instrument that may be used for making payments[6];
- *"the user"*: this is typically a person (natural and/or legal) who (pursuant to a contract concluded with an issuer) holds a payment instrument that may be used for payment.
- *"the acceptor"*: this is typically the trading or service establishment that accepts, on its behalf or on behalf of its network, payment of goods and services by holders making use of a payment instrument;
- *"the acquirer"*: this is typically the (financial) institution that collects transaction information from the acceptor and is responsible for the settlement with the latter.

Given that all schemes rest on a multiplicity of issuers, users, acceptors and acquirers, it is not uncommon for the scheme to rely on mutually agreed procedures for the clearing (i.e. the

[6] In the case of electronic money, the issuer of the electronic money, the issuer of the card, and the institution which makes the card available to the user might be different entities.

transmission, reconciling and confirmation of payment orders) and settlement (i.e. the discharge of obligations as between the parties through transfer of the amounts due) of transactions. In this respect, the role of network operators (e.g. frequently, but not exclusively telecom operators) as carriers of financial information, although not one of direct participation in a payment system, needs to be borne in mind.

3. Information Society and the advent of Electronic Commerce

The global Information revolution, and its most striking examples Internet and the growth of electronic commerce, is already transforming the way in which business and people interact. It has the potential to become the key stimulus for the world's economy into the next century. It appears to have become an important business tool, also affecting every day life. The Internet has therefore the potential of striking initial and transactional costs down to a fraction of the more traditional ways of transacting. This could be particularly true of the financial services industry and, especially, of systems and instruments for effecting payments.

Perhaps more important in the present context is to understand if, and when so how, crime may exploit information technology. The question to be answered is whether the Information Society and, in particular E-commerce, with the consequential enhanced use of information communication systems they bring, are giving rise to new threats or barely accelerating traditional patterns[7].

In the context of its work on the Information Society and Electronic Commerce, the Commission has already launched a number of initiatives, aiming in particular at establishing a clear framework for its further development, so as to stimulate investments in electronic commerce services with ensuing benefits for EU in terms of growth, competitiveness and employment. [8] Urgent progress and successful implementation of these initiatives will no doubt contribute to the establishment of an enhanced security environment, thus ultimately also benefit payment systems and instruments.

---

[7] A study on computer-related criminal activities (the COMCRIME study) has been commissioned by DG XIII and was recently finalised by Prof. Sieber, Univ. Würzburg, and Prof. Kaspersen, Free Univ. of Amsterdam. http://www2.echo.lu/legal/en/comcrime/sieber.html

[8] These initiatives include: the Communication on An European Initiative in Electronic Commerce [COM(97)157 final of 15.04.1997]; the proposal for a European Parliament and Council Directive [COM(97)356 final of 09.07.1997 (97/0198 (COD)] on the Legal Protection of Services based on, or consisting of, Conditional Access; the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions [COM(97) 503 final of 1 October 1997] on Ensuring Security and Trust in Electronic Communication: towards a European Framework for Digital Signatures and Encryption; the proposal for a European Parliament and Council Directive [COM(98)297 final of 13.05.1998] on a common framework for electronic; the Communication on Globalisation and the Information Society – The Need for Strengthened Co-ordination" [COM(98)50 final]; the proposed Action Plan to promote the safe use of the Internet O.J. C 48 of 13.02.1998. , which focuses at increasing confidence in the networks by a number of action lines and is therefore part of activities to further electronic commerce.

4. Criminal law

a) substantive law - types of criminal offences

Criminal legislation in relation to payment instruments is generally based in all Member States on the concept of "forgery" and "counterfeiting". However, these terms do not have the same meaning in all Member States' criminal law. In general, the two elements of these behaviour are the act of making a false instrument or forging a genuine instrument and the fraudulent intent of using it. Some legal systems include other requirements such as the existence of a "substantial effect".

All Member States' criminal legislation have criminalised the counterfeiting of banknotes and coins. As regards traditional paper instruments (i.e. cheques), the divergence between legislation in the Member States is more significant. In relation to payment methods such as payment cards, the difference is even more important. In some countries, to commit the offence, the offender must actually use the means of payment and sometimes even a proof of intent is required. The mere possession of a stolen or counterfeited payment card or the theft of a payment card are not considered as offences in all Member States. Difficulties increase when criminals make, use and possess counterfeited payment cards rather than misuse lost or stolen cards. Most Member States have no laws expressly relating to payment card crime and rely on existing legislation drafted for more classical deceptions using documents which is not fully adapted to technological innovations.

Computer and information technology abuse interacts with fraud related to payments, where the fraudsters utilise an electronic payment system, or indeed whenever the payment transaction is processed electronically. Criminal misuse of computers to defraud the beneficiary of a payment, the payment card industry, or the financial institution is not always covered by existing legislation. Unauthorised access is not criminalised everywhere. Manipulation of data in order to illicitly effect a transfer of funds is not necessarily included in the concept of swindling where this requires deceit or exploitation of a mistaken belief, which could not easily apply in computerised communications.

Criminal organisations exploit such differences and operate from the least protected market. Those differences in Member States' legal systems pose considerable difficulties in the investigation and prosecution of fraud across national boundaries.

A first conclusion to be drawn is therefore that in an attempt to deal with a Pan-European problem, one should avoid making these established terms the departure point, and instead focusing on *the behaviour* giving rise to the problem.

A second conclusion is that any *instrument-based or instrument dependent classification* should be abandoned, in favour of more durable and flexible categories. Indeed, criminal activity is not, a-priori and in itself, instrument-specific. Much rather, criminal offences may be :

(i) directed at the payment instrument itself, and at the security features that enable, restrict and/or protect access to use of the payment instrument,

(ii) directed at the payment transaction itself, including the system for ordering, collection, processing, clearing and settlement thereof, and/or

(iii) related to the means for preparing and carrying on the criminal activity, including the (elaboration of the) device-making equipment.

As a consequence, it is proposed to describe the types of behaviour which should be combated, avoiding the use of established offences while focusing on the target of the offender. This classification should be "intent-related" and "instrument-neutral", so as to avoid too precise a codification of offences, which could be subverted by technology or service innovation and which could lead to divergent interpretations of the offences.

Finally, it is useful to highlight that a behaviour-related approach has already been implemented – and appears to have been largely successful - in the United States, where older criminal legislation for consumer protection related to credit cards combined with newer legislation targeting most types of manipulations with *access devices*, covers all non paper-based payment methods, focusing mainly on remote access products.

b) procedural law

In order for any court to be permitted to pass judgement over the behaviour of a person, the court must be satisfied that it has jurisdiction or right to rule over that person.

In criminal law, the criteria for jurisdiction is normally that the criminal act has taken place on the territory of the State where the court is located, although in some Member States and for some offences the nationality of the offender will be a determining element regardless of where the offence was committed. For most crimes against non-cash means of payment, and particularly systems based upon telecommunications infrastructures, a transaction may cross one or more jurisdictions on its way between the originator (the culprit) and the target (the victim), or vice versa. Depending on how criminal law is constructed in the states involved, jurisdiction can prevail in the sending as well as in the receiving state simultaneously. The opposite may also be true, that none of the States will have jurisdiction, any proposal on approximation of substantive criminal law provisions should therefore be followed by a discussion on the question of jurisdiction, and any discussion on mutual assistance must be preceded by such a discussion.

Cooperation between judicial authorities in criminal matters is mainly effected by providing mutual legal assistance and through extradition arrangements.

In the former case, a Member State that wishes to prosecute for offences but needing evidence from another Member State, can request and receive such evidence from the state concerned. The

arrangements for doing so are mainly based upon bilateral agreements between States and the 1959 European Convention on Mutual Assistance and its protocol. Member States are at present working on a draft European Union Convention to supplement the provisions of the 1959 Convention insofar as they apply to the Member States of the European Union.

The future Convention will seek to improve and make more efficient the applicable procedures. The Action Plan endorsed by the European Council in Amsterdam, in its Recommendation 16, refers to the importance of this work for efficient judicial cooperation in the fight against organized crime.

Extradition arrangements are also in place whereby a Member State can have a person charged with a serious offence or convicted of such an offence returned from another Member State for prosecution or to serve his/her sentence in the Member State concerned. The main instrument that provides arrangements for such cooperation is the 1957 European Convention on Extradition and its protocols. In order to supplement and facilitate the application of this Convention, Member States adopted in 1995 an EU Convention on Simplified Extradition Procedures which provides for a simplified procedure for persons who consent to extradition. The 1996 EU Convention relating to Extradition further improves the conditions applying to extradition between Member States by i.e. making a broader range of offences extraditable by decreasing the threshold of sentence necessary for an offence to be extraditable.

5 International aspects

To ensure that approaches envisaged at the worldwide level is coherent and compatible with that of the EU, it is important that all parties (authorities, industry and users' groups) seek to co-ordinate their initiatives in the relevant international fora and groups, establishing wherever possible global agreements. For instance, following the Halifax Summit, the G-8 set up a Senior Experts Group on Transnational Organised Crime, the so called "Lyon Group". Among its activities, it has discussed the launching of joint projects to investigate and combat particular forms of organised crime. Fraud to payment cards and to other access devices received particular attention in this context. Currently, the Commission is participating in the discussions of all these for a with an objective to avoid unnecessary duplication of efforts and facilitate coordination.

Furthermore, a working group under the Council of Europe (the PC-CY or "Cybercrime" working group) is currently preparing a Draft Convention on Computer-related crimes, in which an important feature is a list distinguishing traditional offences that can be committed in a computer environment (e.g. "swindling"), from new offences, which are intrinsically computer-related (e.g. "hacking").

Apart from ongoing information exchange activities with Countries of Central and Eastern Europe and PHARE-financed projects, it should be noted that the Title VI Programs GROTIUS and OISIN have a potential for financing individual projects directed at improving cross-border cooperation through enhanced knowledge, training and competence of the relevant groups of

practitioners in Member States, and that these Programs are open also to participants from the candidate countries.

Finally, in the context of the pre-accession strategy and Accession Partnerships, consideration is being given to develop programs to take account of policy towards combating organized crime. This could include, where appropriate, the problem of fraud and counterfeit of non-cash payment systems.

6. Towards a Union Policy: sharing responsibilities

In the light of the sections above, the Commission believes that the answer to the problem lies in a common approach, rather than on isolated, partial initiatives. Moreover, the fundamental element of such an answer is that it calls for a sharing of responsibilities amongst all (directly or indirectly) interested parties, within a hierarchy of responsibilities.

First of all, instruments and the underlying systems and features allowing for their use, must be technically suitable as is necessary to reduce the potential scope for criminal abuse. This is by far the "conditio sine qua non" and the first step for an effective response to crime. It must be a primary responsibility of the industry as a whole (and participating financial institutions individually) to strive towards ever more secure payment applications, as it is to clearly disclose to users the actual level of security associated with the different payment products they offer. This responsibility needs to be extended to encompass network operators, on whom it rests to ensure the secure exchange of financial information.

However, there is no doubt that technical security on its own will only help in so far as, and to the extent that, it succeeds in raising the protective threshold. It is not and should not be viewed as the conclusive solution. All actors concerned and authorities must also play their part in promoting and implementing the appropriate framework that will lead :

- to provide incentives for early detection measures (prevention), and
- to establish a safety net designed at sanctioning offenses where these have occurred (sanctions).

Secondly, crime is in no way a geographically constrained phenomenon, even less so in the light of the present prospective information revolution. To enhance the effectiveness of any action, there is a need wherever possible to ensure consistency of approach at international level. This is particularly true of organised crime, which has time and time again demonstrated the ease with which it can conveniently migrate towards and operate from safer havens.

In order to meet the challenge posed by the threats of crime in the form of fraud and counterfeit of non-cash means of payment, the Commission is proposing a draft Joint Action. Its aim is to ensure that fraud involving all forms of non-cash means of payment is recognised as a criminal offence and punishable by effective, proportionate and dissuasive sanctions in all EU Member States, and that appropriate mechanisms of co-operation are put in place in order to prosecute these offences efficiently. This is without prejudice to the faculty for Member States to incriminate additional forms of e.g. computer crime, like the mere unauthorised access to an information technology-based payment system.

The Joint Action deliberately avoids the use of strictly defined qualifications under existing criminal law because they do not cover the same elements everywhere. The approach taken instead is to describe the various behaviour which should be criminal offences throughout the Union in a way which does not limit the Joint Action's application to particular types of non-cash payment instruments. In order to do so, the list of Article 2 is drawn up on the basis of the direct aim pursued by the offender. It looks at the immediate target of the fraudster: whether the attack is directed at the payment instrument or at the making of payment instruments, or whether it is directed at one or more payment transactions, or at the system itself for ordering, collecting, processing, clearing, and settling the payment transactions.

Therefore, the form of a joint action was preferred: it indicates the result to be achieved while leaving to the national authorities the choice of method. The proposed Joint Action has of course been drafted on the basis of the Maastricht Treaty. It will have to be adapted to the new legislative framework and will take the form of a Framework Decision, when the Amsterdam Treaty comes into effect.[9] Under the existing treaty, Article 3 paras 6 and 7 and Article 6, which deal with judicial cooperation, are not formally part of the Commission's initiative. They are submitted for consideration by the Commission in order to complete the text. Finally, the proposal has to be seen in the context of other instruments already adopted or still in the course of discussion like the joint action criminalising the participation in a criminal organisation[10], the Joint Action establishing the European Judicial Network[11] and the draft convention on mutual assistance.[12]

Additional Actions

---

9 This means in particular that Art. 35 of the consolidated version of the Treaty on European Union will apply, which provides that the Court of Justice shall have jurisdiction to give preliminary rulings on the validity and interpretation of Framework Decisions, subject to declarations made by the Member States. It also provides for the possibility of submission of statements of case or written observations to the Court and gives the Court jurisdiction to review the legality of Framework Decisions and to rule on disputes between Member States on the interpretation of Framework Decisions where such disputes cannot be settled by the Council within 6 months of having been referred to it by one of its Members.

10 Draft Joint Action adopted by the Council on the basis of Article K.3 of the Treaty on European Union on making it a criminal offence to participate in a criminal organization in the Member States of the European Union. (not published)

11 Proposal for a Joint Action to create a European Judicial Network (not published)

12 Draft Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (not published).

Furthermore, a set of actions are set out in Annex 2. All interested parties are invited to consider these actions, with a view to taking the necessary measures for their effective implementation. Furthermore, in order to assess clearly what additional measures, including the legislative ones, might need to be taken in this field, the Commission intends to stimulate a wide-ranging debate with all interested parties and encourage them to respond to the issues raised in this Communication. Comments (in writing) to these actions are requested no later than 31 December 1998.

JOINT ACTION
ON COMBATTING
FRAUD AND COUNTERFEITING
OF NON-CASH MEANS OF PAYMENT

EXPLANATORY MEMORANDUM

Commentary of the articles

Article 1

Article 1 contains definitions of terms used in the Joint Action. These definitions are without prejudice to more specific definitions in the Member States.

1. Paragraphs 1 and 2 contain core definitions for the Joint Action. Paragraph 1 defines "*(non-cash) payment instrument*" as described under point 1 before, i.e. including all payment instruments with the exception of bank notes and coins.

2. Paragraph 2 defines "*payment transaction*" as any transaction for obtaining of money or value, making or receiving of payment in respect of goods, services and any other thing of value and/or the issuing of an order involving transfer of funds , through a payment instrument.

3. The definitions include software and are linked to Article 2 (k) which lists prohibited activities related to device-making equipment.

4. The definition of "*legal person*" is taken from the Second Protocol to the Convention on the protection of the European Communities' financial interests[1] .

5. "*money laundering*" is defined as in the Council Directive 91/308/EEC of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering

6. The term "*national*" is to be understood in accordance with declarations made by Member States to Article 6(1) (b) of the European Convention on Extradition of 13 December 1957. The Extradition Convention will apply to serious cases under this Joint Action as referred to in Article 3.3.a.

Article 2

Article 2 describes the behaviour which the joint action proposes should be incriminated in all Member States, if it is not yet the case, and made subject to the provisions set out in Articles 3,4, 5 and 6. The behaviour listed in Art. 2 do not cover mere breaches of contractual obligations.

a) typically corresponds to the theft of cheques or cards;

b) covers, e.g. the creation of completely false cards, as well as the forging of existing ones;

[1] OJ No C 221, 19.7.1997 p. 11

14

c) corresponds to the selling, transmitting, etc., of payment instruments, false or falsified, as well as of genuine instruments, but without authorisation of the legitimate holder;

d) covers the knowing possession of a payment instruments falling under (a) or (b)

e) targets the actual use of a payment instrument falling under (a) or (b);

f) deals with the case where a merchant or a service provider knowingly accept a payment made under the circumstances described under (e);

g) addresses cases where for instance genuine card identification data are used without the authorisation of the legitimate holder to make a payment by phone;

h) covers the case where completely false data are used for the same purpose; it is not to be understood as prohibiting pseudonyms as identification by the legitimate holder;

i) concerns the situation where, for instance, the information circulated within the processing system are intentionally modified so as to direct the order to the benefit of an account, other than the legitimate beneficiary of the order;

j) deals with the case where identification data are transmitted to a person who is not entitled to that information and would or could use them to obtain value or pecuniary advantage;

k) relates to the means for preparing or carrying on one of the criminal behaviours described before;

l) covers the case for instance of possession of specially designed holograms or papers for printing cheques;

m) extends incrimination to anyone who would assist or instigate any of the behaviours previously described or who knowingly benefits therefrom.

Article 3

1. This article requires Member States to review their existing law and practice with a view to ensuring that the measures set out in paragraphs 1 to 7 are achieved.

2. Paragraph 1 provides that the list of behaviour set out in Article 2 should be classified as criminal offences.

3. Paragraph 2 provides that legal persons should be liable for the offences envisaged by paragraphs 1 and 5, committed for their benefit by any person, acting either individually or as a part of the organ of the legal person in accordance with the modalities of national law. This text is modeled on Article 3 of the Second protocol to the Convention on the protection of the European Communities' financial interests but it has been modified so that it does not have the requirement that the person committing the offence should have a leading position in the organisation and does not include liability arising out of lack of supervision or control.

15

4. Paragraph 3 puts an onus on Member States to provide for appropriate punishment of offences. Insofar as natural persons are concerned, the provisions are modeled on provisions contained in the Convention on the protection of the European Communities' financial interests, the Protocol to that Convention and the Convention on the fight against corruption involving officials of the European Communities or officials of the Member States of the EU. Penalties must be effective, proportionate and dissuasive.[2]

In complying with this ruling , the Member States have some discretion in determining the nature and severity of the penalties which may be provided for. These need not always necessarily involve deprivation of liberty. Fines might be imposed in addition or as an alternative to imprisonment .

The article does, however, require Member States to provide for penalties involving deprivation of liberty, which can give rise to extradition, in the most serious cases. It will be for the Member States to decide what criteria determine the seriousness of an offence in the light of their respective legal traditions.

As far as legal persons are concerned, in some jurisdictions the concept of criminal liability of legal persons does not exist. This fact is recognised in Article 4 of the Second Protocol to the Convention on the protection of the European Communities' financial interests and that Article is the model used for this provision but sanctions more appropriate for offences involving Community and national officials have not been included in this text. The requirement is for effective, proportionate and dissuasive sanctions, the minimum obligation is to impose criminal or non-criminal fines.

5. As not all Member States have yet ratified the 1990 European Convention on Laundering, Search, Seizure and Confiscation of the proceeds from crime, paragraph 4 requires Member States to take the necessary measures to make possible the seizure and confiscation or removal of the instruments and proceeds of the offences envisaged by paragraph 1 and money laundering or property the value of which corresponds to such proceeds. Instruments, proceeds or other property seized or confiscated should be dealt with in accordance with national law.

6. The money laundering provisions of the 1990 European Convention is applied to predicate offences in accordance with declarations made by parties to that Convention. The EC Directive is limited to proceeds derived from drug trafficking offences at present although the Directive may in future be extended to all serious crime. Paragraph 5 establishes money laundering related to the proceeds of the offences envisaged by this joint action as a criminal offence. Money-laundering is defined in Article 1 in accordance with Council Directive 91/308/EEC of 10 June 1991.

7. The international nature of fraud to non-cash means of payment means that to combat it effectively rules on jurisdiction and on extradition need to be clear and to be as progressive as national legal systems will allow to guard against persons evading prosecution. For that reason the provisions in this paragraph are modelled on provisions used for forms of crime

---

[2] The expression is taken over from a judgement of the Court of Justice of the European Communities (case 68/88, Judgement of 21.9.1989, ECR.2965) expressed as follows: (the Members States) "must ensure in particular that infringements of Community law are penalised under conditions, both procedural and substantive, which are analogous to those applicable to infringements of national law of a similar nature and importance and which, in any event, make the penalty effective, proportionate and dissuasive."

with particular international dimensions. The models used are the jurisdiction provisions of the Convention on the protection of the European Communities' financial interests, the Protocol to that Convention and the Convention on the fight against Corruption involving officials of the Communities or officials of Member States of the European Union.

8. Paragraph 6 establishes a series of criteria conferring jurisdiction to prosecute cases involving the offences covered by the Joint Action on national enforcement and judicial authorities.

A Member State shall establish its jurisdiction in two situations:

- where the offence is committed in whole or in part in its territory, irrespective of the status or the nationality of the person involved (territoriality principle)

- where the offender is a national (active personality principle). The criteria of their status means that jurisdiction can be established regardless of the *lex locus delicti*. It is up to Member States to prosecute for offences committed abroad. This is particularly important for Member States which do not extradite their own nationals.

However, as not all Member States' legal traditions recognise extraterritorial jurisdiction, Member States may, subject to the obligation under paragraph 7, limit their jurisdictions to the first of these two situations. In addition if they do not do so they can still make the jurisdiction rule in the second situation subject to specific situations or conditions.

9. Paragraph 7 takes account of the fact that some Member States do not extradite their nationals and seeks to ensure that persons alleged to have committed fraud to non-cash means of payment do not evade prosecution because extradition is refused in principle on nationality grounds.

A Member State which does not extradite its own nationals must take the necessary measures to establish its jurisdiction over the offences concerned when committed by its own nationals outside its territory. The offences may have been committed in another Member State or in a third country. In such circumstances the requested Member State must submit the case to its legal authorities for the purpose of prosecution. The provision is not intended to affect national rules regarding criminal proceedings. The requesting Member State must transmit the files, information and exhibits relating to the offence to the Member State which is to prosecute the offence. The requesting Member State shall be informed of the prosecution initiated and of its outcome.

Article 4

The purpose of Article 4 is to provide for co-operation between public and private bodies and bodies involved in the control of payment systems and the authorities responsible for investigation and punishment of the offences envisaged by the Joint Action. Each Member State must take the necessary measures, while respecting its own internal law, to ensure that the bodies concerned advise the relevant authorities where there is reasonable ground for suspecting that an offence has been committed as well as providing all reasonable information and, if appropriate take part as experts in the procedures. This article is modeled on the

provisions of the Joint Action concerning action to combat trafficking in human beings and sexual exploitation of children[3].

Article 5

The purpose of this provision is to clarify that each Member State must ensure that the obligations as they arise from Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data are also met in relation to the processing of personal data provided for in this Joint Action. The possibility of exchange of personal data arises in particular in Article 4. The proposed wording is made pending a forthcoming general discussion of the issue of data protection in Title VI matters.

Article 6

1. The purpose of this Article is to augment instruments on international co-operation to which Member States are a party and which will apply to this Joint Action.

International co-operation between judicial authorities in criminal matters is mainly effected by providing mutual legal assistance and through extradition arrangements.

Mutual Assistance arrangements are contained in a number of bi-lateral and multilateral agreements , notably the 1959 European Convention on Mutual Assistance and its 1978 Protocol, the 1990 Convention on the Schengen Agreement and the Benelux Treaty. EU Member States are at present working on a draft European Convention and a Protocol to supplement the provisions of the 1959 European Convention on Mutual Assistance and its Protocol.

Extradition arrangements are provided in the 1957 European Convention on Extradition and its protocols as well as in the Schengen Convention and the Benelux Treaty. Member States adopted in 1995 a EU Convention on Simplified Extradition Procedures which provides for a simplified procedure for persons who consent to extradition. A Convention signed in 1996 relating to Extradition further improves the conditions applying to extradition between Member States. Both these instruments will enter into force following completion of the national ratification procedures.

Other EU instruments agreed, or planned to deal with organised crime will impact on the fight against fraud to non-cash means of payment. Examples are the Joint Action on the establishment of a Judicial Network to facilitate judicial co-operation between Member States and the Joint Action making it a criminal offence to participate in a criminal organisation.

2. Paragraph 1 requires Member States to afford each other the widest measure of mutual assistance in respect of investigation, prosecution and carrying out the punishment imposed, relating to offences provided for in this Joint Action.

3. When a positive conflict of jurisdiction occurs, paragraph 2 establishes that Member States shall consult one another with a view to co-ordinating their action to prosecute effectively.

---

[3] OJ No. 63, 4.3.97, p. 2

4. Paragraph 3 puts an onus on Member States to ensure that information concerning the offences envisaged by the Joint Action, as well as information on persons convicted of such offences and information useful for investigation and prosecutions is organised in such a way that it is accessible for effective use and exchange with other Member States. This provision is modeled on a similar provision in the Joint Action concerning action to combat trafficking in human beings and sexual exploitation of children[4].

Article 7

This is a standard article which refers to the follow-up and commitment for the implementation of this Joint Action. It establishes that the Council will assess on the basis of a report made by the Commission on the fulfillment by Member States of their obligations by the end of 2000.

[4] OJ No. 63, 4.3.97, p. 2

19

JOINT ACTION

adopted by the Council

on the basis of Article K. 3 of the Treaty on European Union

on fraud and counterfeiting of non-cash means of payment

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article K.3 (2) (b) thereof,

Having regard to the report of the High-Level Group on Organised Crime, approved by the Amsterdam European Council on 16 and 17 June 1997, and in particular Recommendation N° 18 of the Action Plan;

Considering that fraud and counterfeiting of non-cash means of payment often operate on an international scale;

Considering other instruments agreed by the Council such as the Joint Action establishing the European Judicial Network and the Joint Action on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union will also assist in the fight against fraud of non-cash means of payment;

Recognising the importance of the work developed by various international organisations (i.e. the Council of Europe, the G8, the OECD, Interpol and the UN);

Whereas the Council considers that the seriousness and development of certain forms of fraud regarding non-cash means of payment require comprehensive solutions including both repressive measures and preventive strategies based on a sharing of responsibilities amongst the payment system industry, the individual users and the authorities;

Whereas the Commission submitted a Communication entitled "A framework for action combating fraud and counterfeit of non-cash means of payment" which advocates a Union Policy covering both preventive and repressive aspects of the problem;

Whereas this Joint Action is one element of such comprehensive approach;

Whereas in order to achieve approximation of legislation incriminating fraud and counterfeiting of non-cash means of payment, a clear legal instrument is needed;

HAS ADOPTED THIS JOINT ACTION:

Article 1 - Definitions

For the purposes of this Joint Action, and without prejudice to more specific definitions in the Member States' legislation,

1. *"(non-cash) payment instrument"* shall mean an instrument with the exception of legal tender (i.e. bank notes and coins) enabling, alone or in conjunction with another (payment) instrument, the legitimate holder/payer, to obtain money or value, to make or receive payments in respect of goods, services or any other thing of value, to issue an order or message requesting or otherwise authorising the transfer of funds (in the form of a monetary claim on a party) to the order of a payee;

2. *"payment transaction"* shall mean obtaining of money or value, making or receiving of payments in respect of goods, services or any other thing of value, and/or the issuing of an order or message requesting or otherwise authorising the transfer of funds (in the form of a monetary claim on a party) to the order of a payee, through a payment instrument;

3. *"device-making equipment"* shall mean any equipment (including software) designed or adapted for the access, manufacture or alteration of any, or part of any, payment instrument or payment transaction and shall include equipment designed or adapted to change or alter any information or data carried on or in any payment instrument or payment transaction;

4. *"legal person"* shall mean any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations;

5. *"money laundering"* shall mean the conduct as defined in the third indent of Article 1 of Council Directive 91/308/EEC of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering.

6. *"national"* of a Member State shall be construed in accordance with any declaration made by that State under Article 6(1) (b) of the European Convention on Extradition of 13 December 1957.

Article 2 – Description of behaviour

In order to combat fraud and counterfeit of non-cash payment instruments and payment transactions, each Member State undertakes to review their relevant national laws concerning the measures set out in Articles 3, 4, 5 and 6 relating to the following types of behaviour:

a) misappropriation of a payment instrument;

b) counterfeiting or falsification of a payment instrument;

c) knowingly handling, unauthorised by the holder, of a payment instrument;

d) knowingly possessing a misappropriated, counterfeited or falsified payment instrument;

e) knowingly using a misappropriated, counterfeited or falsified payment instrument;

f) knowingly accepting a payment made under the circumstances covered by the previous indent;

g) knowingly unauthorised use of identification data for initiating or processing a payment transaction;

h) knowingly using fictitious identification data for initiating or processing a payment transaction;

i) manipulation of relevant data including account information, or other identification data, for initiating or processing a payment transaction;

j) unauthorised transmission of identification data for initiating or processing a payment transaction;

k) unauthorised making, handling, possession or use of device making equipment for the purpose of:

- manufacturing or altering any payment instrument or part thereof;
- initiating or processing payment transaction, or
- changing or altering any information or data carried on, or in, any payment instrument or transaction;

l) knowingly unauthorised possession of an element or part of a payment instrument;

m) involvement as accessory or instigator in, or knowingly obtaining of value or pecuniary advantage derived from any of the behaviours described above involving a criminal intention.

Article 3 - Measures to be taken at national level

Each Member State shall review existing law and practice with a view to providing that:

1. The types of behaviour set out in Article 2 are classified as criminal offences.

2. Legal persons can be held liable for the offences provided for in paragraphs 1 and 5 committed for their benefit by any person, acting either individually or as part of an organ of the legal person in accordance with modalities to be defined in the national law of the Member State.

3. The penalties for these offences and for intentional participation in or attempt to commit them should:

   a) insofar as natural persons are concerned, be effective, proportionate and dissuasive criminal sanctions including, at least in serious cases, custodial penalties involving deprivation of liberty which can give rise to extradition;

   b) insofar as legal persons are concerned, be effective, proportionate and dissuasive sanctions which shall include criminal or non-criminal fines.

4. The necessary measures are taken to make possible the seizure and without prejudice to the rights of bona fide third parties, the confiscation or removal of the instruments and proceeds of the offences provided for in paragraph 1 and 5, for property the value of which corresponds to such proceeds. Any instruments, proceeds or other property seized or confiscated shall be dealt with in accordance with the national law of Member States.

5. Money laundering related to the proceeds of the offences provided for in paragraph 1 is established as a criminal offence.

6. It establishes its jurisdiction over the offences provided for in paragraphs 1 and 5 where:

   a) the offence is committed in whole or in part within its territory;

   b) the offender is one of its nationals.

   Subject to the provisions of paragraph 7, any Member State may limit the application of its jurisdiction to the rules laid down in paragraph 6.a. A Member State which does not apply such a limitation may nevertheless apply its jurisdiction to the rules laid down in paragraph 6.b only in specific cases or conditions.

7. Where a Member State does not extradite its nationals it should establish its jurisdiction over the offences provided for in paragraphs 1 and 5 when committed by its own nationals outside its territory.

Each Member State shall, when one of its nationals is alleged to have committed in another Member State an offence established in accordance with paragraphs 1 and 5 and it does not extradite that person to that other Member State solely on the grounds of his nationality, submit the case to its competent authorities for the purpose of prosecution if appropriate. In order to enable prosecution to take place, the files, information and exhibits relating to the offence shall be transmitted in accordance with the procedures laid down in Article 6 of the European Convention on Extradition of 13 December 1957. The requesting Member State shall be informed of the prosecution initiated and of its outcome.

Article 4 – Co-operation from public and private services or bodies

Each Member State shall take the necessary measures to ensure that the public and private services and bodies involved in managing, monitoring and overseeing the payment systems, while respecting the internal law of the Member State, will co-operate with the authorities responsible for investigation and punishment of the offenses established by this Joint Action. In particular they should:

- advise those authorities on their own initiative, where there is reasonable ground for considering that one of these offences have been committed;
- provide those authorities with all useful information either on request or on their own initiative;
- if appropriate, take part in the procedures as experts.

Article 5 - Data Protection

Concerning the processing of personal data, this Joint Action shall be implemented so as to ensure a level of protection equivalent to the protection foreseen in the European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Data should be used only for the purposes for which it has been transmitted.

Article 6 - Co-operation between Member States

1. In accordance with applicable conventions, multilateral or bilateral agreements or arrangements Member States shall afford each other the widest measure of mutual assistance in respect of proceedings relating to offences provides for in this Joint Action.

2. Where several Member States have jurisdiction in respect of offences envisaged by this Joint Action, these States shall consult one another with a view to co-ordinating their action in order to prosecute effectively.

3. Each Member State shall ensure that information concerning offences envisaged by this Joint Action as well as persons convicted of such offences and information which could be useful for investigations and prosecutions of such offences is organised in such a way that it is readily accessible and can be effectively used and exchanged with other Member States, subject to national law governing secrecy of proceedings.

Article 7 - Commitment and follow-up

1. Each Member State shall bring forward appropriate proposals to implement this Joint Action for consideration by the competent authorities with a view to their adoption.

2. The Council will assess, on the basis of a report made by the Commission, the fulfilment by Member States of their obligations under this Joint Action, by the end of 2000.

3. This Joint Action shall be published in the Official Journal.

4. It shall enter into force on the date of its publication.

Actions to prevent fraud from occurring

a) The *payment system industry, as a whole, including network operators,* are invited to

1) enhance the security intrinsic to the payment product on offer, the systems for the processing of transactions originated thereby, including the carrier network system,

2) upgrade the security of tools allowing for conditional & discriminatory access to the use of their payment products,

3) set up structures for exchange of information and learn from experience whilst also ensuring a high level of confidentiality and protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy.

Furthermore, the *payment system industry* is invited to

4) set up training programs primarily destined for financial institutions' own staff, as well as the development of the necessary capabilities for systematic reporting of criminal activities to enforcement agencies,

5) promote educational material directed at users of payment products (principally retailers and holders).

The Commission considers that the need for an early detection of criminal offences should in particular be taken into account by the industry when designing the payment instrument and the underlying systems (under 1 and 2), and declaring the (potential) fraud to the structures designed to this purpose (under 3).

Furthermore, to ensure a harmonious and pro-competitive development of the market for payment services, the Commission is of the opinion that attention should be paid to ensuring that actions under 1) and 2) do not lead to an unwarranted hindrance of competition and of the development of the Information Society as a whole, notably through practices amounting to restrictions on access to a system or on freedom to cross-border services, as well as by way of exclusivity arrangements.

b) *Individual issuers as well as individual users (retailers and holders)* are invited to

promote a reasonable and fair apportionment of responsibilities & liabilities between the various parties to a payment system (i.e. between issuer/holder; between acquirer/retailer), which favors:

- compliance with terms and conditions governing issue, use and acceptance of a payment instrument,

- the earliest possible notification procedure.

The Commission thinks that as a general policy goal, it must be a priority to ensure that individual users do not suffer as a consequence of crime occurring in respect of the use of a payment instrument and payment systems, unless it can be proven that they have taken part in the criminal activity. Moreover, in view of the technological aspects which are under the control of the participating (financial) institutions, the burden of proof should not be put on the holder.

Nevertheless, users should be informed concerning the security measures they have to respect, and they should assume, as citizens, a civic duty to participate actively against fraud, notably by the earliest possible notification of the anomalies they note, in particular in the information they receive subsequent to a transaction.

c) *Authorities* are invited to

- coordinate information gathering and awareness raising initiatives, which may include industry.[5]

- assist the industry, individual issuers and users in their efforts towards the achievement of a security environment. At EU level this will involve promoting the establishment across the Union of a supportive regulatory and non-regulatory framework. The Commission has already taken a number of initiatives to this effect.

At the Union level

The Commission stresses that as the existing Community regulatory framework is essentially aimed at creating a Single Market within which financial services, and in particular payment services, may freely circulate.

Furthermore, EC legislation in this field is mainly devoted to giving effective application to the Treaty provisions. This has been achieved by way of coordinating the provisions relating to the taking-up and pursuit of the business of financial institutions. These provisions have been supported by a number of specific provisions harmonizing the basic rules of prudential supervision.

---

[5] The UK recently proposed a Joint Action, for the establishment of a network of contact points in the Member States, to improve exchange of information in relation to credit card fraud. The Interpol General Assembly in October 1997 adopted a proposal to establish a universal classification system for "bad" credit cards, which in reality is a clearing house function for the Interpol Secretariat to collect information, with the assistance of the credit card industry, and disseminate it through the contact lines with national police forced already existing with Interpol. The PC-YC of the Council of Europe has received a Belgian expert proposal for the establishment of contact points in relation to cyber-crime in general.

27

A number of specific Commission initiatives are aimed at an appropriate regulatory framework in the area covered by this Communication.

In this context, the Commission is currently working on a draft proposal which aims to ensure the financial integrity of issuers of electronic money and thereby foster consumers' confidence in this new means of payment.

Furthermore, in the specific context of the Information Society and Electronic Commerce, the Commission has already recently adopted a number of measures including the proposal for a directive on the legal protection of services based on, or consisting of, conditional access and the proposal for a directive on electronic signatures. In addition, in the field of secure payment systems for electronic commerce, the Commission has co-funded several industry-wide R&D initiatives under various information and telecommunications technology programs[6].

The Commission has already recently issued a Recommendation[7] concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, thereby setting out the minimum transparency, responsibility, liability, and redress requirements. The Commission has undertaken to monitor its implementation until the end of 1998. If implementation is not found to be satisfactory, the Commission will propose a Directive in this domain.

Furthermore, the Commission has announced that it also intends to modernise and update an earlier 1987 Recommendation[8] with a view to establishing a clear framework for the relationship between acquirers and acceptors in respect of electronic payment instruments. In this context, the Commission may take into consideration the possibility of applying particular conditions to the collection of payment cards so as to take into account the absence or repetition of fraud. This would contribute to reducing the risk factor of the payment instrument and the underlying system.

---

6 E.g. project AC026 SEMPER - Secure Electronic Marketplace for Europe.

7 Communication from the Commission to the European Parliament, the Council, the European Monetary Institutes and the Economic and Social Committee: "Boosting customers' confidence in electronic means of payment in the Single Market"; COM(97) 353 final of 09.07.1997; O.J. L 208 of 02.08.1997, p. 52.

8 Commission Recommendation 87/598/EEC of 8 December 1987 on a European Code of Conduct relating to electronic payment (relations between financial institutions, traders and service establishments, and consumers), O.J. N° L 365 of 24 December 1987, page 72.

The corresponding Community regulatory framework

The present annex briefly summarizes the key elements of Community law making up the regulatory framework within which financial, and in particular payment services, are offered, mediated and used.

The primary source of law is the EC Treaty. Firstly, as an indispensable precondition for the integration of domestic financial markets and, thereby, a Single Market for financial services, articles 73b to 73g of the EC Treaty introduce the regime of free movement of capital and payments within the Community and in respect of third countries. Secondly, articles 52 (freedom of establishment) and 59 (freedom to provide services) of the Treaty are cornerstones of the Single Market edifice for financial services in that they enable firms respectively to set up (and be authorized) in one Member State, under the supervision of that Member State's authorities, as well as to freely provide services throughout the Community under the single authorization of the Member State of establishment.

The secondary source of law in the field of financial services is embodied in the layer of Community legislation devoted to giving effective application to the Treaty provisions recalled.

This has first and foremost been achieved by way of coordinating the provisions relating to the taking-up and pursuit of the business of financial institutions, notably those of credit institutions, investment firms and insurance undertakings. These provisions have been accompanied and supported by a number of specific provisions harmonizing the basic rules of prudential supervision.

Amongst the directives in the field of financial services is a Council Directive on the prevention of the use of the financial system for the purpose of money laundering[9]. Based on the recognition that money laundering is often carried out in an international context, so that the criminal origin of the funds and its proceeds may be better disguised, the directive sets the basis for international co-ordination of a non-penal nature, placing a number of requirements on Member States: notably, a requirement to prohibit money laundering, requirements on credit and financial institutions to identify their customers and to record transactions exceeding certain amounts, requirements on institutions to examine and report any transactions which they regard as likely to be related to money laundering, and a requirement that authorities responsible for combating this phenomenon co-operate with credit and financial institutions and their supervisory authorities.

[9] Council Directive of 10 June 1991; OJ L 166/77 of 28.6.91.

Although the financial services directives are targeted primarily at the financial service sector, they are also concerned with the rights and interests of consumers. They contain certain provisions that safeguard consumers' rights to correct and complete information, protect their legal interest and provide access to means of redress.

Recently, pressure has been building up to reinforce the concept that the single market for financial services is not just for business. In May 1996 the Commission decided to issue a Green Paper on *Financial services: meeting consumers' expectations* to have a comprehensive debate on consumer policy in financial services. On 26 June 1997, the Commission adopted a follow-up Communication on *Financial services: enhancing consumer confidence*[10]. The Communication announces a series of forthcoming initiatives, some of which have already been launched (e.g. an extension of the recommendation on new means of payment) or are in the process of being launched, including a future proposal on distance contracts for financial services.

[10] COM(97)309 final of 26.6.1997.

ISSN 0254-1475

COM(98) 395 final

DOCUMENTS

EN 09 10

Catalogue number : CB-CO-98-432-EN-C

ISBN 92-78-37888-7

Office for Official Publications of the European Communities

L-2985 Luxembourg