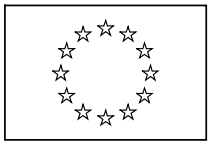

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 2.12.2003
COM(2003) 718 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

concerning a

New Legal Framework for Payments in the Internal Market

(Consultative Document)

COMMUNICATION FROM THE COMMISSION
TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

concerning a

New Legal Framework for Payments in the Internal Market

(Consultative Document)

Executive Summary

Regulation 2560/2001/EC on cross-border payments in euro has contributed to a considerable reduction in the price for cross-border payments in the Internal Market and has provided an incentive for the payment industry to modernise their EU-wide payment infrastructures.

This has been an important step in the process of achieving a Single Payment Area for non-cash payments in the Internal Market, which does not exist despite of the introduction of the euro. However, further progress needs to be made, as technical and legal barriers still prevent EU citizens, companies and payment services providers from reaping the full benefits of a truly integrated area for non-cash payments. The Internal Market for goods and services cannot function properly without cheap, efficient and secure payment services.

The existing legal framework for payments is to a large extent based on national rules which leads to a fragmentation in the Internal Market. This is detrimental to the deployment of EU-wide infrastructures by payment service providers. Community legislation on payments services, mostly applicable to cross-border payments, also needs to be reviewed and consolidated.

The removal of the technical and legal barriers should ensure efficient payment services, competition on equal terms, adequate protection of payment service users, security of payments, and should guarantee legal certainty for all parties concerned in the payment process.

The Communication's aim is to consult all interested parties on the general objectives and principles that should govern the modernisation and simplification of the regulatory framework applying to retail payment services in the Internal Market. This consultation should lead to the Commission presenting appropriate proposals for a New Legal Framework for Payments.

The Communication is accompanied by 21 Annexes raising various specific legal and technical issues concerning the efficient functioning of the Single Payment Area.

Comments on the issues raised in this Communication are welcome before 31 January 2004 and may be sent to: European Commission, Directorate General Internal Market, C107 01/04, B – 1049 Brussels. E-mail address: e-mail: markt-f4@cec.eu.int.

OUTLINE

1. INTRODUCTION

This Communication deals with the legal framework to be proposed in order to establish a Single Payment Area which – despite of the introduction of the euro – still does not exist. This is an important element for the integration of the retail markets in general and retail financial services markets in particular. The Regulation[1] (2560/2001) on the cross-border payments in euro has contributed to reducing considerably the price for payment transactions in the Internal Market and pushed the creation or adaptation of the underlying EU-wide payment infrastructures. This process should be accompanied by the necessary legal framework in recasting and completing the existing legal acts. This is the reason for this Communication.

This Commission Communication invites the general public for comments on the various issues raised in the main text and the Annexes with regard to forthcoming legislation on retail payment services in the Internal Market, henceforth termed the "New Legal Framework". Issues to be addressed concern essential and coherent information requirements to customers, legal rights and obligations of users and providers of payment services, legal certainty in the transaction process, etc. These questions are particularly important for users, both consumers and businesses, for banks acting as payment service providers and the payment card industry.

The issues addressed in the Annexes certainly have for different market participants or under the Internal Market objectives a different importance. However, it is difficult to quantify them and/or to establish a ranking. Most legislative proposals or subjects qualify with variant degree under different objectives as e.g. payment market efficiency, legal or technical security, payment service user protection or Internal Market Integration. The present text reflects the outcome of an extensive public consultation[2] which started in spring 2002. During the public consultation, oral and written comments were received from a broad variety of respondents (national ministries, central banks, consumer associations, individual banks and banking federations, the payment card industry, telecom companies and associations etc.).

This Communication takes account of the comments and suggestions already received. However, in order to validate or correct the Commission's analysis on the different legal issues, it is not sufficient in the forthcoming comments on this consultation to express only preferences for a "way forward" but to deliver strong arguments. It is important to get information about the economic benefits of the various legislative proposals and to avoid over-regulation.

---

1 OJ L 344, 28.12.2001, p. 13.

2 A possible legal framework for the Single Payment Area in the Internal Market – Working Document (MARKT/208/2001); Summary Document (MRKT/4007/2002); Discussion Document (MARKT/F-4/4002/2003).

2. PAYMENT SERVICES AND INTERNAL MARKET

Modern economies based on the principle of division of labour are characterised by efficient payment markets. Payment systems and instruments constitute the invisible financial veil of the real economy. Payment transactions perfect the exchange of claims and liabilities; they are the corollary of the purchase of goods and services, of countless individual decisions on savings and investments or the simple service of sending money.

Payment services are provided by many operators. The smooth functioning of the huge number of daily transactions[3] leads the public to underestimate their economic performance and added value delivered nearly seamlessly at any moment. Sound payment systems and providers contribute to the trust in the currency and to financial stability. In all national economies, the payment service activity employs a considerable number of persons.

The economies of all Member States are equipped with efficient payment systems and instruments. Payments at national level are delivered quickly, securely and at low cost. However, in the EU there is still, to a large extent, fragmentation between national payment markets on the one hand, and cross-border payment markets on the other hand. This is inconsistent with the Internal Market principle [Article 14(2) of the Treaty], since it gives rise to a border effect.

Much has been achieved in recent years to overcome this situation. Most importantly this includes the introduction of the euro, the establishment of TARGET[4] by the System of European Central Banks and the adoption of the Regulation 2560/2001/EC on cross-border payments in euro. All three initiatives have considerably improved the way payments are made in the Internal Market and brought benefits for the EU citizens and the economy in general:

Citizens throughout Euroland use the same euro coins and notes. There is no longer a need to be familiar with and to buy other currencies when travelling. There are no longer foreign exchange charges. No extra conversion calculations need be made when paying for goods and services: there is immediate price comparability. People have already forgotten the former burden and cost; the advantages are taken for granted. For euro cash payments there is a single payment area: Euroland has basically become a domestic cash market[5].

For large value payments in Euroland, since 1999, TARGET has provided similar efficient and expedient services as at national level for inter-bank and commercial cross-border payments.

The Regulation determines that the price for a cross-border payment in euro up to 12.500 euro[6] in the Internal Market should be the same as for the corresponding

---

3 The total number of non-cash payments in the EU in 2001 was 52billions. This corresponds to 143 million transactions per day and meant 138 non-cash payment transactions per inhabitant during one year. Source: European Central Bank – Blue Book.

4 Trans-European Automated Real-Time Gross Settlement Express Transfer.

5 See Annex 17.

6 Up to 50.000 euro from 1.1.2006; the principle applies as well for SEK.

payment within a Member State. This price equality principle throughout the EU is already operational for electronic payments since 1.7.2002 and since 1.7.2003 for credit transfers. The former border effect of considerable price differences has been eliminated[7]. The market for non-cash payments in euro from the payment service user's point of view has to be considered as a domestic market.

Efforts were also undertaken by European banks[8] but their impact on the retail payment markets in Euroland was, until now, rather limited and isolated. The EU payments industry was not sufficiently prepared for the rapid adoption and implementation of the Regulation: the effect of the principle of price equality had – at that time - not found its reflection in the appropriate payment infrastructure which would enable the cross-border payment services to be provided at equal cost.

However, the payment industry has accepted the principle and immediately initialised considerable common efforts. A European Payment Council was established in June 2002. It decided on a wide-ranging work programme for a Single Euro Payment Area with suggestions for considerable changes on how to organise payment services in the European Union. These plans include, in particular, the decision to establish, as a priority a new infrastructure[9] for credit transfers in euro at very low transaction cost and an expedient execution time of three days maximum. Many further actions are envisaged to realise Single Euro Payment Area. Other market players (card companies, etc.) are also actively improving their services and newcomers (e.g. telecommunication operators) are preparing alternative and specialized methods for a more efficient EU payment market.

3. THE REASONS FOR THE COMMISSION'S INITIATIVE

3.1. Need for a general overhaul of the present legal framework

There is general acceptance that the Internal Market for payments in euro has to be considered as a domestic payment market. However, looking at the legal environment of this Single Payment Area, the situation is unsatisfactory. Although there is an "Acquis Communautaire" on EU payments legislation, which allows the Internal Market to be considered as one single jurisdiction, the present legal framework – for the reason stated below - seems to require a fundamental overhaul for payments in the Internal Market.

In accordance with the Commission's policy of "Better Regulation", this Communication lays down the present "state of play" based on long preliminary discussions and preparations for a New Legal Framework for payments in the Internal Market. The Commission's services immediately started after the adoption of the Regulation 2560/2001/EC an intensive review of the present EU payment legislation with all parties concerned in order to address present legal deficiencies, the need to take account of market and technological developments, the Internal Market dimension and other policy objectives. This Communication is a further consultative document aimed at gathering views and comments. The reactions are

---

7 E.g. since 1.7.2002 for card payments and ATM transactions.

8 E.g. Euro Banking Association's (EBA) systems EURO1 and STEP1.

9 EBA's STEP2 made its first transactions on 28.4.2003.

important for the Commission in order to know all relevant arguments and assessments before proposing the most appropriate provisions for a New Legal Framework.

3.2. Lisbon Summit objectives and Financial Services Action Plan

The proposal for a New Legal Framework for payments in the Internal Market has become part of the Commission's Financial Services Action Plan (FSAP)[10] as a key measure and consequence of the recent adoption of Regulation 2560/2001/EC. This initiative focuses its efforts, through an appropriate legal environment, to improve customer convenience and protection and to underpin the efforts of the payment industry for an efficient and safe payment market. It contributes to financial stability and the proper functioning of the economy in the EU. Modern payment infrastructures are contributive to the objectives of the Lisbon Summit conclusions for making Europe the world's most competitive, knowledge-based economy by 2010.

3.3. Internal Market arguments

3.3.1. Removing legal barriers and uncertainty

The liberalisation of capital has facilitated cross-border money transfers within the EU but the Internal Market, in particular for retail payments, is still not as efficient as at national level. Differences also exist between national legislations and conventions with regard to payment services in the Internal Market. The New Legal Framework should remove, where necessary, these legal barriers to a Single Payment Area, especially if they create an obstacle to the proper functioning of EU-wide payment infrastructures and systems as, for instance, the rules relating to the revocation of a payment order differ depending on where the order was placed in the Internal Market. Interoperability, the use of common technical standards and harmonisation of the essential legal rules are paramount.

Legal uncertainty is an element hindering payment service providers and users from transacting without reticence or at all. This is, for example, the case for direct debit transactions, which do not yet exist at EU-level (see Annex 16). This is particularly the case for regular, recurring payments (e.g. standing order for a foreign newspaper or a public utility for a summer house in another Member State) for which 'domiciliation' is not possible. If the users, e.g. consumers and SMEs, should reap the full benefit from the Internal Market, cross-border payment services have to be as efficient as those at national level.

The New Legal Framework should therefore deliver in this respect and enhance customer confidence and welfare in a Single Payment Area in the Internal Market.

3.3.2. More efficiency in a larger market

Some present Community acts on payments apply only to cross-border payments others to all payments. EU integration has sufficiently progressed and the Internal

---

[10] See 6th Progress Report of the Financial Services Action Plan (FSAP), which is available on the following address: http://europa.eu.int/comm/internal_market/en/finances/actionplan/.

Market should also include an integrated payment market. The intention of the payment industry is to create a Single Euro Payment Area. Consequently, the existing legislation should be reviewed in this respect and, as far as necessary, the New Legal Framework should cover all payments, national and cross-border, with the same legal provisions. The New Legal Framework should considerably simplify the necessary EU legislation compared to the present situation, for instance, in the case of the existing rules on cross-border credit transfers (see notably suggestions under Annex 14). This will be in the interest of the payment service providers and users alike. The realisation of New Legal Framework and Single Payment Area will also create the potential for improved payment efficiency (see Annex 15), since this should result in a consolidation of the payment infrastructure with a much higher number of transactions than in each individual Member State. Economies of scale can result in lower transaction costs, thereby counterbalancing the present strain put by the Regulation's price equality principle or even allowing for still lower prices.

3.3.3. Enlargement

Although the New Legal Framework will not be in place at the time of the accession of the new Member States, the enlargement is an additional reason why the discussion on the legal framework is necessary. The transposition of the "Acquis communautaire" into payment legislation has added, through the transposition procedure in these candidate countries, new national legislation to the already existing diversity of national rules in the 15 Member States. Such national diversity creates legal differences which may easily become obstacles to the proper functioning of the Internal Market. The question should be addressed as to whether directly binding EU rules could be more appropriate (see section 3.5 below).

3.4. Simplifying and improving of implementation of EU-legislation

The present EU legal provisions on payments are contained in different types of EU legal instruments: a Regulation (2560/2001/EC) introducing the equality of charges for cross-border intra-EU payments in euro and corresponding national payments, which is directly legally binding without transposition into national law; a Directive (97/5/EC)[11] facilitating cross-border credit transfers in establishing some customers' protection requirements, which had to be transposed into national law to become applicable; a Recommendation (97/489/EC)[12] providing for the protection of customers using electronic payment instruments, such as payment cards, which – although not a legally binding instrument – was supposed to be fully implemented and applied in the EU. The co-existence of the three key legal acts is confusing[13] since several provisions overlap. Certain rules of the Directive have become obsolete after the adoption of the Regulation[14]. A recent Commission Report[15] on the

---

11 OJ L43 of 14.2.1997, p. 25.

12 OJ L208 of 2.8.1997, p. 52.

13 E.g. all three legal acts contain measures with regard to the information to be provided. This is confusing for both the payment industry and the consumers: the payment services users have no easily understandable set of requirements. The payment service providers are equally in a situation where they have to refer to various legal texts with similar requirements but expressed in different terms, without knowing whether the information they provide is sufficient under EU and national law.

14 See e.g. Annex 14.

Directive demonstrated shortcomings. A Study[16] on the Recommendation 97/489/EC revealed insufficient transposition into national legislation. The Recommendation already announced the intention of the Commission to propose binding legislation. In conclusion, a "recasting" of the existing legal framework for payments appears necessary.

3.5. Implementing new money laundering requirements in the payments area

The Financial Action Task Force (FATF)[17] adopted on the 14th of February 2003 interpretative notes on two Special Recommendations on Terrorist Financing (Special Recommendation VI on "money transmitters" and Special Recommendation VII on "originator information")), which both deal with payment issues. The Commission is supportive to integrating these requirements into Community law and the New Legal Framework is the appropriate place to legislate. The payment industry claims fully EU harmonised rules on these aspects: this is considered to be important in order to ensure a level playing field (equal conditions for payment service providers, access, cost of compliance etc.) and for reasons of efficiency ("identical originator information requirements to allow straight-through-processing (STP). The question as whether this is best achieved through an EU Regulation needs to be addressed (see section 4.6 below and Annexes 1 and 8).

3.6. Taking account of new technological and market developments

The landscape for payments is in a state of radical upheaval due to the general technological and market developments. It is important to examine whether existing payment legislation is still sufficient and appropriate to deliver the framework for the market and its participants.

Payment service users consider that some payment transactions - notably in the present technological environment - should be offered at a marginal low price and in near real time. Under these conditions, cash payments - still mostly offered freely to the individual person by mutualising the cost to society - are likely to be increasingly replaced by modern non-cash payment means. Many citizens appreciate the convenience of these modern instruments if they provide appropriate security and protect their interest. This holds in particular in the context of e-commerce and distance selling modes, but applies also in point-of-sale and other face-to-face payment situations. Many new media services are increasingly offered against the payment of very small amounts (micro-payments). Vendors of these goods and services require automated, secure payment processing methods to keep their administrative tasks to a minimum and with assurance for the irrevocability of the payment. The Commission is strongly interested in proposing the essential - necessary and sufficient - legal provisions for payment service users in the Internal

---

15 Report from the Commission to the European Parliament and to the Council on the application of Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers (COM/2002/0663 final).

16 The Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer (May 2001) is available on the following address: http://europa.eu.int/comm/internal_market/payments/.

17 See FATF homepage: www.oecd.org/fatf.

Market, taking into account these developments. Such provisions should basically deal with security, information and legal certainty requirements.

Payment service providers are mostly aware that some traditional payment instruments and systems are no longer economically adequate, effective, user-convenient and fast enough. The transaction nature of the payment service is increasingly coming to the forefront of management considerations on efficiency and profitability. Immense investments - notably in information technology - have been made by the banks at national level. The need to benefit from economies of scale through high payment transaction volumes has triggered new forms of co-operation and consolidation of payment infrastructures. Interoperability has called for common technical standards and conventions beyond the national level, notably in order to realise Single Euro Payment Area.

In addition, technological developments, cost considerations and compliance with customer convenience has brought about a profound review of the existing payment instruments. A clear shift to alternatives and the emergence of new payment methods compared to classic credit transfers or cheques is taking place (e.g. direct debit, cards, internet- , e- or m-payments). These developments are often being supported by business proposals of many new players in the payments market in response to topical new or alternative payment needs as e.g. micro-payments in the internet or m-payments. The "mushrooming" of newcomers in the payment market has been accompanied by their often quick disappearance because of the lack of critical payment transaction mass. This Communication invites comments and ideas in order to improve the legal environment for existing and potential payment service providers (see in particular Annex 1) Issues to be addressed cover market access and pursuit of business conditions.

4. THE GUIDING PRINCIPLES FOR A FUTURE PROPOSAL FOR A NEW LEGAL FRAMEWORK FOR PAYMENTS IN THE INTERNAL MARKET

Further to this consultation, when drafting a formal proposal for a New Legal Framework, the Commission intends to observe some guiding principles which are considered particularly relevant in the context of EU payment legislation. The most important principles are dealt with in this chapter.

Attention is drawn also to the Annexes which, in several cases, already contain formulated legal text elements as "possible ways forward" in drafting a forthcoming legal proposal of the Commission. However, it should be noted that no decision has been taken to definitively propose legal rules in these cases nor any formulation of the text. It is important to receive comments on the implications of such provisions. This Communication also addresses, in a piecemeal way, those forthcoming legal issues which have been identified until now. The final Commission proposal for the New Legal Framework for payments in the Internal Market will carry the present "acquis communautaire" provisions, as far as necessary, in a comprehensive legal text.

4.1. Efficiency as a permanent objective

In a recent report[18] of the Committee of Payment and Settlement Systems it is stated: "Retail payments systems and instruments are significant contributors to the broader effectiveness and stability of the financial system, in particular to consumer confidence and to the functioning of commerce" and "Public confidence in the currency could be endangered if retail payment systems were inefficient, impractical for users and unsafe". Efficient payment instruments and methods are essential to all relevant parties in a commercial relationship, in particular for the consumers and the retail trading sector.

For exactly these reasons efficiency of payment systems and instruments should be a concern and guiding principle for the EU legislator when proposing and deciding on a New Legal Framework for payments in the Internal Market. This is not only an essential objective, but a very practical requirement in order to meet the general expectations of payment service users, notably with regard to the security, price and execution time of payments.

Payment service providers undertake considerable efforts to permanently improve their business proposals, accentuated by competitive pressures and innovation. The Single Euro Payment Area work-programme of the European Payment Council is a clear move in this direction with regard to euro payments in the Internal Market. Card companies, telecommunication operators and others are also committed to come up with new offers.

The main contribution for the New Legal Framework is an examination of the present legal environment for payments in order to identify legal or regulatory barriers hindering improvements in the efficiency of payment markets, systems, service providers and instruments. Such legal impediments for payment efficiency can exist as a result of disproportionate legal requirements on market access (see Annex 1) or for the deployment of a payment instrument or innovative techniques, in legal provisions creating insufficient legal certainty or in unnecessary reporting obligations etc. The New Legal Framework is supposed to address these questions. This Communication invites all interested parties to provide comments to the Commission.

4.2. Security as a "conditio sine qua non"

Without a high level of security of payment systems and instruments, there will be no trust on the payment service user's side and therefore little use of unsafe payment methods. However, there is no such thing as a totally secure payment means; even cash can be lost, stolen or counterfeited.

The development of more and more sophisticated payment systems/instruments renders their security assessment increasingly technically complex. For the sake of profitable payment business and maintaining at the same time trust in their products, payment service providers are strongly self-interested to keep payment services as safe and uncompromised as possible. There is, however, a trade-off between the

---

[18] Bank for International Settlement, Committee of Payment and Settlement Systems, Policy issues for central banks in retail payments, Basel, March 2003.

degree of security and the cost for the protection against misuse, mostly in the form of fraud and counterfeiting. Payment service providers and fraudsters were, in recent years, involved in a permanent race in this area, with the result that security solutions moved generally to a very high level of protection.

The Commission considers it a high priority to enhance payment security and to contribute to the fight against payment fraud (e.g. payment card fraud, fraud on e-banking). Although the implementation of the most economically feasible security infrastructure for payment services is a task and a responsibility primarily belonging to the payment industry, the New Legal Framework should address the issue of legal security of the payment environment. This includes the security evaluation of payment systems and instruments, the legal safeguards in the case of non-, defective- or unauthorised execution of payment transactions or of non-access to payment services as e.g. in a breakdown of the payment network. The legal requirements for digital certification of payments, but also measures to combat fraud, counterfeiting and terrorism financing in the context of payments, are questions to be examined. EU legislation already requires Member States to criminalise fraud and counterfeiting of non-cash means of payments.[19] Other legislative and non-legislative measures are under examination in the context of the three-annual Fraud Prevention Action Plan[20] and the implementation of the FATF Special Recommendations (see section 2.5). The Commission is, in the context of the New Legal Framework, interested to receive views on the desirability of additional legislative security measures and the costs and benefits involved.

4.3. Competition: access to markets and level playing field

The implementation of competition policy in the anti-trust area will be enhanced from May 2004 when Regulation 1/2003/EC will apply and EU rules will be applied uniformly and directly in all Member States. The aim of increased competition is to allow markets to deliver benefits for users. Payment markets are characterised by a large number of payment service providers and users. Most payments operations have to rely on interoperable infrastructures in order to be executed. In addition, the payment service is a transaction business which is inherently susceptible to economies of scale: the cost of a payment transaction decreases with the increasing volume; the fewer the commonly used infrastructures, the higher the economies of scale. Creating and operating infrastructures for these purposes often implies agreements between competitors. Agreements in the financial sector are subject to the same EU competition rules as for other sectors. They can be permitted under certain conditions (for example where the results could not be obtained on a stand-alone basis) but are kept under scrutiny (for example to ensure that new competitors are not prevented from entering a market or that agreements do not result in a de facto pricing policy). There is no need for the New Legal Framework to go into detail on these but such agreements will continue to be subject to normal monitoring and if necessary, investigation.

---

19 See Council Framework Decision (2001/413/JHA).

20 See Communication on Preventing Fraud and Counterfeiting on non-cash means of payments [COM(2001) 11 final].

Low cost operation of payment services can notably be achieved by automatisation and straight-through-processing. This presupposes, however, a high degree of standardisation and agreements on common standards. The introduction of such standards should generally be led by the industry on a voluntary basis. However, a balance must be struck in the public interest between the extent standards are needed to achieve the critical mass for straight-through-processing and interoperability and the possible adverse effects of the creation of standards which might possibly restrict innovation, for instance by creating an incentive to harmonise pricing and/or dissuading new entrants to enter payments markets. The Commission is, in principle, reticent to become involved in the standardisation of payment processing but strongly interested that progress is achieved.

An important aspect of competition in the payment sector is that of open access to infrastructures in an environment which is evolving under the impulse of technological changes and market forces.

In most Member States the exercise of payment service activities is conditional to the possession of a banking or e-money licence but not in all. This differentiation of market access conditions between Member States is detrimental to the functioning of the Internal Market: it is very difficult for payment service providers who operate legally in countries without a licence requirement to gain access to the markets of Member States which insist, for prudential reasons, on a licence. Although under the new Special Recommendation VI of the FATF [in order to combat terrorist financing and money laundering] each payment service provider must in future be registered or licensed, the question of a single EU passport for payment service providers with a simple registration in one Member State remains. Several such money transmitters and other newcomers (e.g. telecommunication operators) have complained that meeting the requirements under a banking licence – designed for the full range of banking activities – is too expensive and burdensome for simple payment service providers and is disproportionate given the reduced risks of such an activity. This raises the general question as to whether competition in the payment market might not be enhanced as a result of a reassessment of the level of access conditions and other – notably reporting – requirements for payment services only. The Commission services are in particular examining this question with regard to mobile operators and are interested in receiving comments. Any decision in this area should, however, respect the level-playing field: same activity, same risks, same requirements.

4.4. Customer[21] protection at a high level

Consumer protection is an important aim behind any legislation on payment markets, providers and instruments. The payment industry too is interested in offering viable business models and payment products that payment service users want. In the Internal Market, consumer confidence in payment transactions is in particular relevant since there is often a cross-border dimension and since confidence is essential when using the potential of e-commerce within the larger EU-market. Article 153 of the Treaty therefore requires a high level of consumer protection, which is a guiding principle for the New Legal Framework. However, the costs for

[21] By customer is meant consumers and other persons, such as retailers and SMEs, using payment services.

such protection need to be assessed since they will ultimately be borne by the customer in one or the other way. In addition one has to take account of the opportunity costs associated with the perceived lack of confidence in some payment means.

There are a whole range of customer protection issues to be addressed in this context and most of them are dealt with in detail in the Annexes. They are all extremely important and can be summarised by the following list:

Focused, coherent and user-friendly information requirements prior and post execution of a payment transaction. Many provisions already exist in present EU payment legislation in this respect which need to be reviewed. One of the most difficult tasks is to strike the right balance with regard to the content and volume ofinformation so that the payment service user reading it, is able to understand and to be aware of his rights and obligations.

Legal safeguards protecting the customer in cases of non-, defective- or unauthorised payment transactions. This is directly linked to the issue of payment security, but questions of burden of proof and the extent of liabilities need to be raised.

Legal safeguards need also to be considered in the distance commerce environment, the emerging use of direct debit payment systems or in cases of non-access to electronic payment systems, etc.

Possibility to have alternative dispute resolution in cases of complaints. Directive 97/5/EC already provided for such systems in cross-border cases and the FIN-NET cooperation network has been established. The New Legal Framework should generalise these possibilities for quick redress for all payments in the Internal Market.

EU citizens expect to make or receive payments relying on simple, familiar payment legislation. The payment service users are basically interested in making expedient and safe payments at low cost. Transparency and convenience are essential. This is also the case for the retail trading sector acting as payment service users.

The Commission's services have also studied proposals to require payment account number portability as in the field of telecommunications. Based on the experience in the Netherlands and UK, but also having regard to the recent compulsory introduction of the common International Bank Account Number (IBAN) as a consequence of Regulation 2560/2001/EC, this idea would result in high costs and be counterproductive. On the other hand, it appears that customers from time to time complain about excessive prices for transferring or closing a payment account. The Commission invites comments as to whether and how the New Legal Framework could regulate this latter problem.

Finally, the Commission's services are discussing with the stakeholders a project called "Card Stop Europe", which aims to provide a simple (if possible 3-digit) single phone number in order to block quickly EU-wide lost or stolen payment cards, with the payment industry and other interested parties. This is one of the suggestions in the Fraud Prevention Action Plan. The main problem is whether such a project

could be realised on a cooperative basis between those companies providing such a service at national level, or whether regulation is necessary.

A high level of consumer protection is also one of the objectives of the EU legislation on data protection[22]. It is necessary to balance the interest of data protection with other needs, such as the prevention, investigation and prosecution of payment fraud cases.

4.5. Legal provisions need to be technically neutral

Particular attention should be given in the forthcoming legal provisions to guaranteeing a level playing field for payment service providers, to ensure technical neutrality with regard to the different payment instruments, to avoid unnecessary payment product harmonisation and not to inhibit innovation. The legal framework should, generally, not "favour" one instrument over another. Competitive advantages based on investments in new technology should be a result of market choice – not a result of legal provisions.

4.6. Recasting of payment legislation must add value

The recasting of EU payment legislation for the Internal Market needs to be done with care and in accordance with the Commission's principles of "Governance[23]" and "Better Regulation[24]". Wide-ranging, overarching payment legislation could be counter-productive, creating unnecessary complexity and disproportionate compliance costs that, generally, will inevitably be passed onto the payment service users individually or together.

Any legislation must add value in terms of financial stability, payment market efficiency (including the Internal Market dimension), payment security and payment service users' convenience. Although it is rather difficult to establish fully conclusive and objective cost/benefit assessments, the overall welfare objectives need to be observed.

4.7. The nature of a future legal instrument

Another question concerns how to proceed. The EU legislator can adopt regulations and directives and the Commission can adopt recommendations. The Commission can also promote co-regulation[25] and encourage self-regulation[26] by market participants. For each issue, the appropriate legal instrument should be selected in the

---

22 See Recital 10 of Directive 95/46/EC on the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, OJ L 281, 23/11/1995 p. 0031-0050.

23 See Communication on Action Plan "Simplifying and improving the regulatory environment (COM/2002/0278 final).

24 See Communication on European Governance: Better lawmaking (COM/2002/0275 final).

25 Co-regulation is defined as a mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (e.g. economic operators, the social partners, non-governmental organisations or European associations).

26 Self-regulation is defined as the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (codes of practice, sectoral agreements, etc.).

light of the criteria mentioned in section 4.5. The question of one or several legal instruments needs to be addressed (e.g. a regulation complemented by some non-binding rules in the form of recommendations). EU legislation could, in addition, be adopted by the Council and European Parliament or by the European Central Bank within its Treaty powers.

When the choice in favour of an EU legal instrument has been made, it should be recalled that the Stockholm European Council invited the Commission "to consider the more frequent use of Regulations where this would both be legally possible and would help to speed up the legislative process". The question for the New Legal Framework is whether the payment market, the payment service providers and users are often not better off with a directly legally binding EU regulation as an outcome of the recasting.[27] The payment industry, for example, invited the Commission to implement the FATF Special Recommendation VII by a regulation for reasons explained under section 3.5. Payment service providers must have a strong interest in knowing conclusively the comprehensive list of essential (necessary and sufficient) legal requirements in order to comply and act under conditions of legal certainty (e.g. on information requirements which must be given to their customers). This also establishes a level playing field but should not prevent any service provider to offer more on a voluntary basis.

Likewise, as Eurobarometer surveys[28] demonstrate, consumers in Europe are very much in favour of clear, comprehensible and essential rules at a high level on their rights and obligations at EU level. UK research concludes, in addition, that e.g. the information to be given to consumers on financial services should be focussed and limited, so that it is read at all. An EU regulation could contribute considerably to solving these problems of legal clarity and simplicity because - since there would be no transposition into 25 national legislations - the risk of diverging national legal texts would be eliminated. Notably payment services users, a retail financial service already widely used cross-border, have a preference in knowing and having the same protection wherever they make a payment transaction in the Internal Market.

5. SCOPE OF PAYMENTS COVERED BY THE NEW LEGAL FRAMEWORK FOR PAYMENTS

The New Legal Framework should in principle apply to all domestic retail payment instruments which are important for the Single Payment Area. Domestic payments in the Internal Market refers to both "national" and "cross-border" transactions, excluding those destined to or arriving from third countries. The focus should be on payment instruments which are provided and used as alternatives to legal tender, i.e. notes and coins. They comprise basically credit transfers, direct debits, card payments and various payments made via electronic means in both circumstances, face-to-face or remote. Specific purpose payment instruments, which only have a limited usability, such a petrol cards etc. may not need to be addressed at EU-level. If these specific purpose payment instruments were to develop and fulfil the criteria of

---

27 In any case, according to EU rules, an EU legal instrument can only be modified by an instrument of the same or higher order. (e.g. a directive by a new directive or by a regulation).

28 See, for instance, Eurobarometer survey 175 "Views on Business-to-Consumers Cross-border Trade" on their homepage: http://europa.eu.int/comm/public_opinion/.

a general-purpose payment instrument, they would obviously fall under the relevant provisions of the planned legal instrument.

Cheques are left outside the scope of the New Legal Framework[29] since they are principally used at national level in most Member States. Their processing is relatively costly and their use increasingly discouraged. The argument is even stronger for cross-border payments by cheque, for which the prices are high, due to traditional handling methods. There is no prospect that this will change.

Very specific instruments, such as bills of exchange, money market instruments and commercial papers, the main purpose of which is generally not to pay, are also excluded from the scope.

The rules to be established in the New Legal Framework should be neutral – as far as possible –with regard to the different payment instruments. Innovation and new means of payment which compete with those covered should also be integrated. The advent of new payment services using electronic means or communication techniques is likely, as there remains a need for micro-payments, interoperable e-purses in euro etc.

Payment services covered under the New Legal Framework should be those provided as a business activity to the public by natural or legal persons (payment service providers). The rules of the New Legal Framework apply to individual and bulk payments. For individual payments, the possibility should remain of agreeing on a contractual basis, specific bilateral arrangements between the payment service provider and user. The individual transaction may be denominated in one of the EU currencies and should not exceed the equivalent of 50.000 euro. However, there may be a need for exceptions or special rules for non-euro currencies.

6. COOPERATION WITH THE EUROPEAN CENTRAL BANK

The preparation and consultation of the New Legal Framework has always been carried out – as far as possible – through discussions and close cooperation with the European Central Bank (ECB). Both, the ECB and the Commission, have for many years been committed to improving the functioning of Single Payment Area. While the focus of the ECB is more on Euroland and the euro large-value and retail payment area, the Commission's attention is focussed on the Internal Market. Both share the common objective that European retail payment systems and services should provide the same service level as they already provide at national level or as already exists for large value payments since the introduction of the euro.

The Treaty confers powers to both the Community and the ECB[30] to regulate (retail) payments, subject to the division of powers in the Treaty. The privilege of the ECB lies clearly in the area of payment oversight and more technical rules with regard to safety and efficiency of payment processing. The Commission's role, in taking

---

29 See Article 3 of Regulation 2560/2001/EC.

30 See Article 22 of the Statute of the ESCB and the ECB. In addition, in accordance with Article 105(4) of the Treaty and Article 4 of the Statute of the ESCB and the ECB, the ECB has always to be consulted on any proposed Community act in its field of competence.

initiatives and making legislative proposals for payment markets, is more in the area of general framework rules in particular relating to the protection of payment service users. In the context of the New Legal Framework, it is the intention to continue the close cooperation and to review this question bilaterally in the light of the outcome of the consultations.

7. THE NEED TO INVOLVE ALL STAKEHOLDERS

The considerable efforts undertaken under the New Legal Framework and in particular by the European payment industry (Single Euro Payment Area etc.) will only result in a satisfactory outcome if all parties concerned contribute.

Contributions start with the comments regarding this Communication and will continue through participation in the forthcoming discussions and initiatives. Already now, it is of the utmost importance that e.g. the payment industry provides and the payment originators use IBAN[31] and BIC[32] as requested in Regulation 2560/2001/EC. Payment service providers and users are not just the banks and their normal private banking clients. The payment service users comprise notably all initiators of bulk and often recurring payments as they exist in public services (e.g. utilities, tax authorities, e-government services) but also in private companies issuing mass payments.

Active involvement of all stakeholders pays off in more efficient payment systems in the Internal Market of the future.

8. NEXT STEPS

The Communication serves to the preparation of the New Legal Framework for Payments in the Internal Market. The main text and the Annexes address a whole range of issues on which the Commission seeks views. Reaction is sought before 31 January 2004 and should be sent to:

European Commission
Directorate General Internal Market
Unit MARKT/F-4
C107 01/04
B – 1049 Brussels
Tel. +32.2.295.47.49
Fax +32.2.295.07.50
e-mail: markt-f4@cec.eu.int

[31] International Bank Account Number.
[32] Bank Identifier Code (SWIFT code).

ANNEXES

TO COMMISSION COMMUNICATION CONCERNING A

NEW LEGAL FRAMEWORK

FOR PAYMENTS IN THE INTERNAL MARKET

LIST OF ANNEXES

Annex 1: RIGHT TO PROVIDE PAYMENT SERVICE TO THE PUBLIC

- ***What is the problem/issue?***

Who can provide payment services in the European Union? Today the rules are very different from one Member State to another[33]. Due to such differences, there is no clarity, neither on the freedom to provide payment service nor on a single passport system with mutual recognition for payment services in the Internal Market, except for those undertakings which provide these services with a credit institution or an electronic money institution license.

Because of rapid technological development, some uncertainty exists in the market as to whether or not a provided payment service would fall under the existing Community legislation and thereby benefit from a passport (e.g. telecommunication operators´ pre-paid services). In addition to this legal uncertainty, there are also the newcomers in the market, who provide or would like to provide payment services but regard the existing legal framework as inappropriate and too burdensome for their activity.

The text presented below does not constitute a literal interpretation of the existing Community legislation, such as the definition of e-money or deposit taking activity. However, some guiding principles and ideas for possible solutions are included in order to promote an open discussion on the best way forward. In particular, two kinds of payment categories are raised in this respect: money remittance services and "special" purpose payment services, such as pre-paid and post-paid small value accounts used for third party payment services[34].

The issue of money remittance needs to be addressed at EU-level as no common approach exists for this kind of payment activity[35]. A licensing regime, valid for the entire EU territory, may therefore be needed. Also the FATF Special Recommendation VI on alternative remittance[36] stipulates that jurisdictions should require licensing or registration for money remittance services. According to this recommendation, such an activity without a license or registration has to be subject to sanctions.

Presently there are few undertakings which would provide e-money as defined in the E-Money Directive[37]: a prepaid payment system where the monetary value issued circulates

---

33 Undertakings providing payment services are subject to very different legal requirements from one Member State to another. In many Member States payment services provided as a business activity have traditionally been restricted to undertakings with a credit institution licence. In relation to recent market developments, the situation appears to be very different from one country to another. The same activity undertaken by a Payment Service Provider may need a licence as a credit institution in country A, an e-money licence in country B, a special license in country C and is considered as an unregulated activity in country D. A table of rules related to the right to provide payment services (MARKT/4007/2003 – Final Draft) is found on DG MARKT homepage http://europa.eu.int/comm/intern_market/payments/ .

34 Third party payment services are in this context considered as the fact to collect payment for a third party.

35 See above-mentioned table (MARKT/4007/2003).

36 See FATF homepage www.oecd.org/fatf.

37 Directive 2000/46/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions (the Directive) was adopted on 18 September 2000. According to Article 10 of the Directive, Member States were required to take the

as a real bearer instrument from holder A to holder B to holder C and so forth. The objective of the E-Money Directive was to cover monetary value circulating as an electronic surrogate for coins and notes between separate individuals, either in an open communication network, such as Internet, or from one electronic device to another in face-to-face transactions. The development of such schemes has not taken place as had been expected before the adoption of the Directive. This has been a result of technical and economic feasibility problems. In addition, schemes which are more or less close to real e-money systems are today mainly operated by undertakings which hold a credit institution license.

However, payment services do exist, which may be regarded as not being covered by the E-Money Directive and which could have a potential to become EU-wide schemes in fulfilling some payment needs, such as micro payments in the internet or in wireless communication services. Some payment products on the market, such as mobile operator accounts and virtual accounts (e.g. PayPal), are closer to credit transfers in a centralised account system than real bearer instruments.

New players, interested in providing small value payments (e.g. micro payments) for some specific purposes, consider the existing prudential rules as too burdensome and not appropriate for their activity. They argue that these rules were established either for a much wider range of risks (credit institution activity) or for payment services which could become surrogates for notes and coins (e-money activity).

Given the existence of a wide range of new payment services and the needs in the market, the Commission considers it important to analyse what would be the right legal framework for these services. This analysis should be based on the prudential risks involved, which need to be further elaborated in this context. Three possible solutions are set out below in order to receive views from all interested parties on the best way forward. Any solution should be based at least on the following three principles:

- all payment services should be covered by appropriate consumer protection rules;
- the prudential requirements should be proportionate to the risks involved;
- the level-playing-field principle should be respected i.e: same activity, same risks, same rules; and
- all payment services should fulfil the relevant conditions relating to the smooth functioning of payment systems.

- ***Possible way forward***

The first solution would be to apply the Internal Market principle of mutual recognition to all kinds of payment activities in the EU. According to the Treaty rules (Art. 49) on the freedom to provide services in the Internal Market, a legally exercised activity in one Member State can ipso facto be legally exercised in other Member States, except if the general interest justifies the contrary. For example, if the Commission takes no initiative for the licensing of money remittance, each Member State will keep or create its own regime: State A considers that this activity needs a banking license, State B only a simple registration. A company

---

implementation measures no later than 27 April 2002. Only 7 licences until now have been granted (UK 1, NL 3, DK 3), some of them to bank subsidiaries.

registered in State B may have the right to provide this service also in State A, and it may be questioned whether State A may oppose to this. Any restriction on the freedom to provide services has to be appropriate, necessary and proportionate. A proportionality test may result in establishing that - under the Internal Market principles – a Payment Service Provider who wishes to undertake cross-border money transmission would be able to do so.

In order to underpin the importance of the mutual recognition principle, the Commission, in its recent Communication[38] on the Internal Market Strategy, has announced a new Directive on services for an effective implementation of that principle.

However, to apply the mutual recognition principle on the basis of the general provisions of the Treaty without establishing harmonised minimum requirements for payment services might bear the risk of disputes before the European Court of Justice. .Mutual recognition might be easier to achieve by establishing an EU-Passport regime based on minimum licensing or registration requirements, for payment services.

A second solution would therefore be to introduce a third specific category of licensing for payment activities. The idea would be to establish a hierarchy of risks among Payment Service Providers: some activities with a fully-fledged credit institution license (funds from the public not exclusively used for payment activities), an e-money institution license (e-money used as an alternative to coins and notes) and a payment institution license (funds from the public exclusively for payment services/transmission).

In such a way a special license or registration for "payment-services-only" could be created without the same level of prudential rules as required by the Credit Institution Directive or the E-money Directive, as there is no evidence that the simple payment transmission activity would require such extensive prudential regulation. Some oversight by central bank and/or supervision by competent authority may, however, be needed. Such activity should, of course, respect any relevant consumer protection and anti-money-laundering rules.

This new license should, in addition to the credit institution and the e-money institution license, create a mutual recognition regime for the Single Payment Area. It could cover one or more situations such as: money transmission services, prepaid and stored value accounts used for third party payments and not covered by the e-money regime and other third party payments services e.g. based on billing.

A third solution would be to adapt the E-Money Directive to the market changes, which were not foreseen at the time of its adoption. One way to do this would be to transform the Directive into a framework directive ("Payment Institutions Directive") regulating the prudential aspects of all payment services which are provided on the basis of customers´ money. This could be done in a similar way to that suggested in the second solution, by establishing different categories of payment services. The aim should be to regulate the requirements for payment services within two legal instruments at EU-level, thereby guaranteeing an appropriate prudential regime and giving legal certainty to these undertakings.

It would also in this case be possible to allow exemptions for certain very specific payment services, such as limited purpose payment instruments or payments which are an integral part

---

38 COM(2003) 238 final dated 07/05/2003 p 12.

of another service (e.g. Premium Rate Services[39]). For these very specific payment instruments without tangible risks, some or all provisions could be waived, if necessary. These possible exemptions should be applicable at EU-level and not only at national level, which is the case with the existing E-Money Directive, as no barriers for payment services should be established in the Internal Market. For instance, a public transport company, which has been granted a waiver for a limited purpose payment instrument in one Member State, should have the right to provide this service also at a station located in another Member State.

If the transforming of the E-Money Directive into a general "Payment Institutions Directive" with necessary modifications were to be regarded as premature at this stage, the Commission may wait for the outcome of the review of the Directive during 2005[40] before proposing any amendments. The drawback of such a postponement is that this would not remove all the existing legal uncertainties for markets participants.

The Commission services welcome views on the importance of further harmonisation of the conditions relating to the right to provide payment services to the public. Views on possible effects on customer protection and market efficiency (competition) are particularly sought.

---

[39] Premium Rate Services are those where the charge for the call or text message is higher than the standard rate, and part of the revenue for the call is passed to a third party.

[40] Article 11 of the E-money Directive requires the Commission to present a report (by 27 April 2005) to the European Parliament and the Council on the application of the directive.

ANNEX 2: INFORMATION REQUIREMENTS

- ***What is the issue/problem?***

Awareness is a crucial element of consumer protection. The Payment Service User needs to have clear information about the payment service which he wants to use, and/or which has been provided to him. Transparency is a pre-requisite in order to be able to compare different offers on the market, to decide on the conclusion of the contract with full knowledge of its terms and conditions, and to be in a better position to understand the service provided. The Payment Service Users should have the same high level of essential (necessary and sufficient) information wherever they buy or use their payment service in the Internal Market.

Furthermore, transparency enhances competition in payment services. Harmonised essential information requirements at EU-level would facilitate the supply of payment services across the Internal Market and reduce the burden for Payment Services Providers to apply diverging national rules and thereby increase competition by creating a level-playing field.

Current information requirements for payment services are spread over different Community texts with a non-uniform content. Because of the non-binding nature of the Recommendation 97/489/EC, not all its information requirements are implemented by the Member States.

- ***Possible ways forward***

Many interested parties have, during the preliminary consultation, expressed broad support for harmonised information requirements for payment services in the Internal Market. In this respect, the quality and not the quantity of the information was regarded as the crucial factor. According to some views, the diversity of products (instruments and services) throughout the Internal Market has to be taken into account. Some of the respondents therefore concluded that the new information requirements should focus on general principles. Some respondents from the banking industry regarded self-regulation, such as a Code of Conduct, as the appropriate means to achieve this at EU-level. Others preferred binding legislation.

The Commission is sceptic that self-regulation would be the appropriate way forward in order to harmonise information requirements in the Internal Market, as this would require the commitment from all players – numerous banks and non-banks - providing payment services. Therefore the Commission services regard binding rules at EU level as more suitable to realise a Single Payment Area. Even the use of a directly applicable instrument, e.g. a Regulation, in order to guarantee the same level of essential protection all over the Internal Market could be considered. The determination of an exhaustive list of essential information requirements would be helpful for the Payment Service Provider and the Payment Service User likewise in terms of legal certainty and transparency. This approach would not prevent an individual Payment Service Provider to give additional information at his discretion or if requested.

In addition, the Commission is of the opinion that the general provisions should, in principal, cover all retail payment services provided to the public and falling under the scope of the new legal act. However, some specific provisions applicable only to certain payment services, such as credit transfers or micro payments, may need to be considered.

A very first draft of provisions, applicable to all payment services, could read as follows:

"1. In good time before the Payment Service User is bound by any contract or offer, the Payment Service Provider shall communicate to the Payment Service User on paper or in another durable medium available and accessible to the PSU all the contractual terms and conditions (hereinafter "the conditions").

2. The conditions shall be set out in writing, including where appropriate by electronic means, in easily understandable words and in a clear and readable form.

3. Any modification of the conditions shall be provided in the same way as indicated in paragraph 1 and 2 and not less than one month in advance of the date of its application. The Payment Service User is deemed to have accepted the modifications of the conditions if he has not terminated the payment service contract up to the date of application.

4. The conditions shall include at least:

(a) a description of the payment service, including where appropriate the technical requirements with respect to the Payment Service User´s communication equipment authorised for use, and the way in which it can be used, including the financial limits applied, if any;

(b) a description of the Payment Service Provider's and Payment Service User's respective obligations and liabilities relating to the provision and use of the payment service; they shall include, where appropriate, a description of the reasonable steps that the Payment Service User shall take to keep safe a payment instrument and the means (such as a personal identification number or other code) which enable it to be used;

(c) where relevant, the period within which the Payment Service User's payment account will be debited or credited, including; the execution time and the value date, or, where the Payment Service User has no payment account with the Payment Service Provider, the period within which he/she will be invoiced. The start of that period must be clearly indicated;

(d) the types of all charges payable by the Payment Service User . In particular, this shall include, where relevant, details of the following charges:

- the amount of any initial and annual fees,

- any commission fees and charges, including the manner of its calculation, payable by the Payment Service User to the Payment Service Provider for particular types of transactions,

- any interest rate, including the manner of its calculation, which may be applied;

(e) where relevant, the reference exchange rate used for converting foreign currency transactions, including the relevant date for determining such a rate.

(f) the period of time during which a given payment order can be contested [revoked, rejected] by the Payment Service User and all practical instructions for exercising this claim;

(g) an indication of the redress and complaints procedures available to the Payment Service User and the method of gaining access to them;

(h) any contractual clause on of the law applicable to the contract and/or the competent court; and

(i) in which language or languages the Payment Service Provider, with the agreement with the Payment Service User, undertakes to communicate during the duration of the payment service contract.

5. Subsequent to a transaction, the Payment Service Provider shall provide the Payment Service User, in the same way as indicated in paragraph 1 and 2, unless the latter expressly foregoes this, with at least the following information:

(a) a reference enabling the Payment Service User to identify the transaction, including, where appropriate, the information relating to the beneficiary;

(b) the amount of the transaction debited or credited on the Payment Service User payment account;

(c) the amount of any fees and charges applied for particular types of transactions;

(d) where relevant the execution time and value date applied; and

(d) where relevant the exchange rate used for converting foreign currency transactions."

The Commission services would welcome views on the impact of the above described draft provisions. Views on the possible effects on customer protection and market efficiency are particularly sought.

ANNEX 3: NON-RESIDENT ACCOUNTS

- ***What is the issue / problem?***

EU citizens complain about different treatment between resident and non-resident accounts within the Internal Market. In particular, citizens have difficulty in understanding different pricing policies, even after the introduction of the euro, given the basic principle of non-discrimination in the Treaty.

Differences between resident and non-resident accounts are made (1) with regard to the opening of accounts, (2) with regard to the running of accounts and (3) with regard to payments from and to accounts.

However, not all Member States have specific legislative or administrative provisions which prescribe a different treatment between non-resident and resident accounts, as there are no specific rules[41]. Others still maintain specific reporting requirements with regard to non-resident accounts for statistical reasons and also for reasons of taxation. These differences in legislation are often used by banks as justification for different prices.

The fact that not all Member States need to provide for a different legal regime for resident and non-resident accounts raises the question as to whether there might be a possibility to remove as many differences as possible within the Internal Market.

- ***Possible Ways forward***

Not all of the above-mentioned problems can be solved within the New Legal Framework for payments, which will have to concentrate on payment-related issues. It is not the intention of this initiative to abolish possible obstacles with regard to the opening of resident accounts.

There may be a need to maintain specific rules for non-resident accounts as such, for example which may be necessary in order to take account of the agreements on the taxation of savings at the ECOFIN this spring. According to this agreement, banks will be obliged to report annually the interest earned by non-residents. Given this decision on withholding tax, it seems less likely that non-resident accounts as such will disappear within the EU.

However, this agreement should have no impact on reporting requirements for *payments* from and to non-resident accounts and serve as a justification for different prices. The latter should be abolished as far as possible. Regulation 2560/2001 already provides the legal basis. Under the principle of price equality for national and cross-border payments and taking into account that payments from and to non-resident accounts are treated like cross-border payments, the Commission sees no justification for banks within the Internal Market to treat euro-payments from and to non-resident payment accounts up the 12.500 euro differently to those from and to resident payment accounts.

However, the banking sector still regards some existing and new reporting requirements for payment transactions as too burdensome. Whether and how far remaining reporting requirements discriminate European citizens because of their nationality and/or residence and

---

[41] Further information can be found in document "National rules related to non-resident accounts" (MARKT/4006/2003 - Final Draft) - http://europa.eu.int/comm/internal_market/payments/.

whether those rules impair the proper functioning of payment systems will be examined. Contributors to the Communication may therefore describe in detail, which existing reporting requirements they regard as inappropriate or too burdensome. Comments on other perceived obstacles in the context of the management of non-resident accounts and their impact on payment services within the EU are also welcomed.

Annex 4: VALUE DATES

- ***What is the issue / problem?***

The value date is the reference date for the calculation of positive or negative interest related to a payment[42] Value dates are generally applied by banks in the context of a wide range of payment orders (credit transfers, cash withdrawals, etc…), as a result of which an account is debited or credited. The value date then determines the reference date for the calculation of interest and, indirectly, the effective availability of the funds. In this way, value dates are used as a complex pricing tool which could include elements of pricing of the payment service and / or remuneration of the money on the account.

The banking community considers that value dates are one element in the bank-customer relationship which should be left to contractual freedom or self-regulation. It is not the objective of this exercise to interfere into issues of the price policy of market players. However, in the ambit of the New Legal Framework for Payments, this request for self-regulation or contractual freedom for value dates has to be assessed with a view to ensuring the efficiency of payments in the Internal Market.

It would be in the interest of both, banks and their clients, to operate in full transparency as regards the use of value dates. Clients could benefit from a more transparent charging system, whereas banks could take advantage from harmonised rules in the Internal Market, for the sake of the proper functioning of infrastructures (e.g. CREDEURO), straight-through-processing and legal certainty.

Legal context

The use of value dates is currently unregulated at EU level, both for national and cross-border payments, with the exception of transparency requirements for cross-border credit transfers in Directive 97/5/EC and for electronic payments in Recommendation 97/489/EC. In some countries (Belgium, Germany, Austria and France), the use of value dates is regulated by national law or case-law, which establishes, most of the time, that value dates should coincide with the transaction or booking date. As regards predominant market practice, there are differences between Member States and payment instruments, but again, for the majority of payments, value dates coincide with transaction or booking dates. This could indicate that the adoption of such practice as the norm for payment transactions would probably not entail major difficulties for most banks. The New Legal Framework, which will apply to all

---

[42] There are different definitions in national legislation. All establish a link between value dates and interests.
Definition in Belgian Law:
"La date de valeur d'une opération bancaire est la date à laquelle un montant retiré cesse de produire des intérêts ou celle à laquelle un montant versé commence à produire des intérêts (Loi du 10 juillet 1997, modifiée par la loi du 19 avril 1999).
Definition in French Case Law:
"La date de valeur est celle à compter de laquelle l'opération inscrite est économiquement prise en considération pour le calcul des intérêts débiteurs, ou, dans les cas où une rémunération est concevable (blocages, comptes sur livret…), pour le calcul des intérêts créditeurs".
Definition in German Case Law:
"…(…) Wertstellung, d.h. der Festlegung des Kalendartages, für den der Überweisungsbetrag in den für die Zinsberechnung maßgebenden - fiktiven – Zwischensaldo des Girokontos eingeht (….)…." (BGH, Urt. V. 6.5.1997 – XI ZR 208/96).

payments throughout the EU, could be used in order to harmonise existing practices and establish a level playing field.

Efficiency of payment systems

When, in the past, most payments were not processed instantly, the use of value dates could be justified for technical reasons. Nowadays, this is generally not the case. Most operations are processed electronically.

The use of value dates may not also be compatible with the objective of improving the efficiency of cross-border payment systems and providing legal certainty as regards the execution time:

- Post value-dating of payments may lead to increasing the de facto execution time, whereas the objective of the single market for payments is to limit the execution time to the minimum required. Such use of value dates may even lead to exceeding the limit established by Directive 97/5/EC. This may be rather exceptional, but not unrealistic as studies have demonstrated. In addition, the beneficiary of the transfer is only informed about the value date of the amount that has been credited to his account a posteriori, while the originator of the transfer receives no notification, which hinders legal certainty as regards the exact execution time.

- Taking into account that there is an intention to further reduce the maximum execution time of cross-border credit transfers in the ambit of Single Euro Payment Area, the question becomes even more acute. CREDEURO, set-up with the objective of reducing the maximum execution time to 3 days (2 days for the sending bank and one day for the receiving bank), would allow little room for the use of value dates, i.e. where value dates were different from the actual booking date.

- Another risk of manipulating value dates in a cross-border context is the pre-dating of the money transferred to the beneficiary's account. In the report on the application of Directive 97/5/EC, this practice has been reported in cases where the maximum execution time was exceeded. This constitutes an illegal circumvention of the obligation established by Directive 97/5/EC as regards execution time.

Transparency

The cost of a payment should be set in a transparent way and allow comparability. Only when transparency and comparability are ensured can the market function effectively. Even if value dates are specified in advance, customers are often unaware of the way they function and do not fully understand its pricing mechanism. This additional price element is not always clearly understood by customers, as the impact of value dates on pricing is difficult to assess. The problem is therefore that value dates introduce an additional non-transparent layer in the structure of tariffs, and as a consequence, render price comparisons difficult. The use of value dates can thus be assimilated to a "hidden tariff". Customers are therefore suspicious as regards the use of value dates, and banks themselves could benefit from increased transparency in their relationship and their standing with customers.

The Commission services would welcome views on the impact of the draft provisions described below. Views on the possible effects on market efficiency are sought in particular.

- ***Possible ways forward***

Although contractual freedom and self-regulation are in general the preferred options, there are a number of arguments which indicate that the use of value dates which are different from the transaction or booking date could be considered to be incompatible with the requirements of price transparency, sound competition, the efficiency of cross-border payments and consumer protection.

The Commission therefore considers two alternatives:

maintain a system of self-regulation but at least regulate transparency in the use of value dates for payments;

or

regulate, in a harmonised manner, the use of value dates in the context of payments. In this case, legal provisions applicable to all payments could read:

Article on the definition of value date

"The value date is the reference date used by the payment service provider for his customer for the calculation of negative or positive interest."

Article on the use of value dates

The value date related to a payment transaction shall not be different from [the date at which the money flow of the payment order at the relevant payment service provider takes place][the booking/transaction date].

Annex 5: PORTABILITY OF BANK ACCOUNT NUMBERS

- ***What is the issue/problem***

In the field of telecommunications, the principle of the portability of telephone numbers has been introduced into Community legislation: the customer can change the telephone operator, while keeping the same number. This measure is regarded as an essential element to enhance competition: the obligation to change the telephone number when changing the telephone service provider was a considerable barrier. The Commission raised the idea of introducing such an initiative in the field of bank/payment accounts during the pre-consultation on this Communication.

The preliminary answers to this consultation concentrated on two aspects: the usefulness and the practicability of portability of accounts.

As regard usefulness, it was underlined that the fact of being able to keep the same payment account number was much less useful than in the Telecom sector. In most cases, it is the Payment Service User who decides to give his number to an institution for a once-off or a recurring payment transaction. The portability could be useful only in the latter case.

As regard practicality, studies carried out in some Member States (UK, NL) where this question of portability has been analysed have shown that the just recently introduced[43] EU-wide IBAN and BIC numbering system cannot work with such a system without incurring excessive costs, provoking problems for efficient straight through processing.

- ***Possible ways forward***

As a result of the preliminary consultation, the Commission does not intend to introduce legal measures aiming at creating portability of banking account numbers. The balance between the practical problems which would need to be solved and the advantages which would arise for the Payment Service User does not justify a portability solution. In addition, they are unlikely to bear the costs of such an operation.

Nevertheless the BIC+IBAN numbering system appears to be a very complicated system and may need to be simplified in the long-run. Therefore the Commission advises the banking industry to launch studies in order to create, in the long run, a more simplified numbering system for credit transfers in the Internal Market.

Many respondents have indicated that greater competition can be achieved through measures aimed at facilitating customer mobility (see Annex 6).

[43] Regulation 2560/2001/EC.

Annex 6: CUSTOMER MOBILITY

- ***What is the issue / problem?***

In the vast majority of cases, a payment is based on a bank account and can only be executed from the bank account. The use of various means of payments is a service which is offered in many cases in connection with the management of a bank account.

In a competitive economy, it is important that the customer is informed of the price for each means of payment in order for him to be in a position to choose. However, sometimes payment service users prefer or need to change the provider. Customers are generally not very mobile because changing a customer-bank-relationship can be a complex operation in case there is the need to inform a whole series of third parties and to re-establish automatic payment orders. In addition, the Commission received from time to time complaints about excessive costs for closing or transferring a payment account.

During the preliminary consultation on the New Legal Framework, many parties stressed the need to improve customer mobility. Proposals made on how to achieve this objective were, however, diverse.

- ***Possible way forward***

It is probably necessary to study in more depth the reasons which are at the origin of the hurdles that a customer encounters when changing a banking/payment relationship. One of these obstacles may be the information which needs to be given to the customer's various debtors/creditors.

It is possible to imagine that all the administrative issues related to the move of an account are executed by a third party. For example, in the Netherlands, the clearing system (Interpay) has a pre-eminent role in the transmission of information from the old account to the new one. Another possibility is that cooperation between banks should allow a smooth transition. It is the option chosen by the British Bankers' Association which stipulates in its code: "7.2 If you decide to move your current account to another financial institution, we will provide them with information on your standing orders and direct debits within five working days (Reducing to three working days from 1 August 2003) of receiving their request to do so".

As regards the administrative issues (e.g. sending of information on the clients' standing orders to the new bank), the Commission considers that improvements in mobility should be introduced by industry through self-regulation. This process will be monitored and the issue may be raised, if needed, by the Commission.

Nevertheless consumer representatives have underlined that the main hurdle is the amount of fees for closing an account. Some examples have been given of so-called "administrative fees" up to 80 euro only for the services relating to the closing of an account. Can such a barrier to mobility and to competition be justified? Such amounts are excessive and not related to the administrative cost, but are established as a brake to mobility.

As regards fees for closing an account, the Commission considers that excessive fees are a barrier to mobility. To close an account is a normal event in a lifecycle of an account. At least full transparency on these fees should be provided to the customer at the time of the opening of an account. Less preferable solutions would be to disallow any closing fees or to set a reasonable upper limit for these fees. The Commission services invite, however, all interested

parties to come up with concrete suggestions which would facilitate customer mobility in payment services.

Annex 7: THE EVALUATION OF THE SECURITY OF PAYMENT INSTRUMENTS AND COMPONENTS

- ***What is the issue/problem?***

At present, payment instruments and components (chip cards, terminals, etc) are certified by the competent authorities before being put onto EU national markets. They are tested with procedures established by the national certification bodies but which are not harmonised at EU level (methodology; type and number of attacks, etc). The result of different testing procedures is that:

- Full comparability is not achieved between similar items (e.g. two different terminals) tested in different Member States. It is thus difficult for the banks, the merchants and the consumers to know to what extent a product is more secure than another. This situation has an impact on buyers' decisions and does not foster users' confidence.

- Certification in one Member State does not mean automatically recognition in the others, as Member States may require different or additional security requirements. In this case, the country with the "stricter" requirements will not recognise a certification carried out in another. This situation is not an incentive to interoperability and is not in line with one of the basis principles of the Internal Market.

- Certification that needs to be undertaken in many countries takes longer and is substantially more expensive. If mutual recognition were to apply in full, the overall certification costs might be reduced and the savings made by the manufacturers could be reflected in the price of the components, with lower costs for banks, merchants and consumers.

Attempts to find objective ways to evaluate the security of payment instruments have been made, namely with moves towards the establishment of standardised security requirements (CC/PP methodology)[44]. There seems to be broad support for the introduction of this methodology, but in practice it is not being implemented expediently.

- ***Possible ways forward***

Concerning the evaluation of the security of payment instruments and components, there is general support for the introduction of the CC/PP methodology in the EU. However, during the consultations in preparation for the present Communication a consensus was expressed against the need for legal provisions to support its introduction. According to the payment

---

[44] The most relevant example are the Common Criteria/Protection Profiles (now ISO standard IS 15408). In this process, the Common Criteria (CCs) are combined with the Protection Profiles (PPs), which are security objectives related to specific categories of instruments (e.g. smart cards). In the PPs, the security features are evaluated against all the threats that a product and its environment face. Assurances about the security level are given by acknowledged certification bodies, which generally operate under the oversight of an evaluation authority. The certification bodies provide a common evaluation scheme based on common accreditation criteria and testing methodology. PPs on smart cards and other components are being developed in the European Union and in the United States under initiatives of the payment industry and government agencies.

industry, legal provisions might increase the costs of payments and jeopardise future developments and innovation. Work on standardised security requirements would better be left to market participants[45]. On the other hand, if legislation were to prove necessary, respondents considered a Recommendation from the Council and European Parliament or from the Eurosystem as a better alternative than EU legislation. Governments and Central Banks encourage a structured and co-ordinated approach for security evaluation that might avoid high costs and time-consuming procedures. They underline that security issues may be addressed through their oversight role on payment systems and means of payments, which should cover the evaluation and certification of products and systems.

Security evaluation is essential in order to maintain confidence in payments and it is necessary to remove obstacles to the mutual recognition of security evaluations of payment instruments and components in the Internal Market. Therefore the Commission needs to examine in more detail the question of mutual recognition, also in the light of the work already undertaken in the mutual recognition of products. To achieve this objective, the Commission may act as a catalyst in order to clarify the issues at stake, and may reconsider its stance altogether if a harmonised methodology to evaluate security, reduce manufacturing costs and significantly enhance consumers' and merchants' confidence in payment instruments is not implemented within a reasonable timeframe by the combined efforts of market participants and other regulators.

The Commission services invite, therefore, views on the importance of this issue. Especially descriptions on any existing problems relating to the mutual recognition are welcomed.

[45] One relevant industry initiative is, for instance, the project called CAPTIN (IST-2000-31034) supported by the IST Programme of DG INFSO. The project is aimed at creating an open communication standard for the on-line interactions between terminals and acquiring (or even issuing) server systems.

Annex 8: INFORMATION ON THE ORIGINATOR OF A PAYMENT (SRVII of FATF)

- ***What is the issue / problem?***

The FATF[46] adopted 8 Special Recommendations on combating terrorism financing in October 2001, in addition to the existing 40 general Recommendations on money laundering. One of these recommendations (SRVII) introduces obligations for financial institutions and money remitters regarding information about the identity of the originator accompanying the transfer. The aim of SRVII is to prevent terrorists and other criminals from having unfettered access to money transfers to move their funds and to detect such misuse when it occurs. An Interpretative Note[47] on SRVII was published in February 2003, according to which all jurisdictions have a two year period to implement the recommendation.

The transposition of SRVII into binding legislation in the EU could be done in several ways. The main issues to consider in this respect are the following:

(1) Should SRVII be transposed by EU legislation or by national legislation?

(2) Scope: which type of payment transactions should be covered?

(3) Which information regime should apply: minimum information (see paragraph 1 of the draft article) or full information (see paragraph 2 of the draft article)?

(4) Need for derogations from the full information regime in the case of "batch" transfers?

(5) Need for exemptions\thresholds?

- ***Possible ways forward***

The Commission proposes to transpose SRVII directly through binding Community legislation, as this would ensure uniform rules throughout the Internal Market. Uniform rules are necessary in order to guarantee the smooth functioning of credit transfers within an efficient payment infrastructure in the EU. A directly applicable legal instrument, such as a Regulation, would therefore be preferable in this respect. The European banking industry has for this reason requested that this issue should be addressed at EU-level.

The Commission is of the view that:

– all credit transfers and money remittance services should to be covered in line with the Interpretative Note

– person-to-person payments executed by means other than traditional credit transfers, such as those offered by card schemes, should also be covered, as they may be regarded as "new means of credit transfers"

---

46 Financial Action Task Force on Money Laundering.

47 See Interpretative Note to Special Recommendation VII: Wire Transfers (http://www1.oecd.org/fatf/TerFinance_en.htm).

With regard to the information which should accompany a transfer, the Interpretative Note provides different rules for so-called "domestic transfers" (inside one jurisdiction) and "international / cross-border transfers" (between two jurisdictions). If each Member-State in the EU were to be considered as one jurisdiction in this context, different rules would be applicable to "cross-border transfers" (between two Member States) and so-called "domestic" transfers (within one Member State). This would be against the above stated objective of the smooth functioning of credit transfers in the Internal Market. This would also ignore the considerable "acquis communautaire" of payment legislation or the objectives of the New Legal Framework for Payments. The Commission is therefore of the opinion that the EU should be regarded as one jurisdiction in respect of the transposition of SRVII. Consequently, considering the EU as a single jurisdiction, the Commission proposes to apply the notion of "domestic transfers" in the sense of SRVII to intra-EU transfers and the notion of "international transfers" to transfers between the EU and third countries.

Another option could be to consider the EU as a jurisdiction, but to apply the full information regime also to intra-EU transfers. The Commission nevertheless sees no justification for such an approach, which would put an unnecessary burden on payment service providers, taking into account the close cooperation already established between judicial bodies in the EU. However, a decision on the minimum information regime would not prevent the use of the full information regime in individual cases.

According to SRVII, batch transfers between the EU and other jurisdictions should be treated as "domestic transfers", instead of "international transfers", and should therefore be subject to the minimum information regime. However, it would be difficult in practice to apply minimum information regime to batch transfers between the EU and third countries, as it is hardly feasible that full originator information is provided in three days to the beneficiary’s institution or appropriate authorities in a different jurisdiction outside the EU. Due to these problems the Commission considers that "batch transfers" should not be treated differently from "non-batch transfers". This would not be in contradiction with SRVII, as it would only imply that the more stringent regime would also be applicable to "batch transfers" originated from the EU to another jurisdiction.

The Interpretative Note allows for the possibility of a "de minimis threshold" (not higher than $3.000) for the payment services falling under SRVII. It is up to each jurisdiction to apply a threshold or not. A mandatory threshold would have the disadvantage of introducing different treatment between two categories of credit transfers, below and above the threshold, which might be detrimental to the efficient functioning of payment systems. Another possibility would be to have an optional threshold, which the payment industry could freely choose whether or not to apply, subject to interoperability and straight-through processing in the Single Payment Area not being impaired. A threshold may be justified for small value payments, such as micro payments.

Based on the above reasoning, the Commission considers that SRVII could be transposed into binding EU-legislation in the following way:

Article on originator information accompanying credit transfers[48] and transfers sent by money remitters

(1) "Credit transfers executed within the EU, except those indicated in paragraph 2, shall always be accompanied by the originator's account number or a unique identifier allowing the transaction to be traced back to the originator.

If requested, the originator payment service provider shall make available to the beneficiary payment service provider [and appropriate authorities], within three business days of receiving the request, full originator information as referred to in paragraph 2.

(2) All other credit transfers and transfers made by money remitters shall always be accompanied by:

- the name of the originator,
- its account number, or in the absence of such a number, a unique identifier allowing the transaction to be traced back to the originator
- the address of the originator, or alternatively the date and place of birth, a customer identification number or a national identity number.

(3) The requirements in paragraphs 1 and 2 shall not apply to credit and money remittance transfers, if the amount executed does not exceed (…euro).]

(4) Credit transfers and transfers sent by money remitters to the EU from third countries having exempted, through their implementation of Special Recommendation VII of FATF, full originator information from accompanying the transfer [batch transfers or transfers below a fixed threshold], are not covered by the present Article.

(5) Where technical limitations at the level of an intermediary payment service provider prevent the transmission of full originator information from accompanying credit transfers or transfers executed by money remitters from third countries (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary payment service provider of all the information received from the ordering payment service provider.

(6) Beneficiary payment service providers should have effective risk-based procedures in place in order to identify any transfers covered by this Article which lack the required originator information. Where appropriate, a beneficiary Payment Service Provider may consider restricting or terminating its business relationship with a Payment Service Provider that fails to meet the obligations specified in this Article.

(7) Member States shall ensure that the compliance of payment service providers with the rules of this Article is monitored effectively."

---

[48] "Any transaction carried out on behalf of an originator person (both natural and legal) through a payment service provider by electronic means with a view to making an amount of money available to a beneficiary person at another payment service provider".

The Commission services invite views on the approach, especially on the possible effects on market practise and efficiency are sought.

Annex 9: ALTERNATIVE DISPUTE RESOLUTION

- ***What is the issue / problem?***

Alternative Dispute Resolution provides extra-judicial procedures for resolving civil or commercial disputes[49]. It is also used in the area of payments. The main justifications for the use of Alternative Dispute Resolution are the limitations at legal costs and the acceleration of the resolution of disputes via arbitrage and mediation.

The advent of the Single Market has increased the movement of persons, goods, services and also payments across the European Union; this has led to an increase in cross-border disputes and the need to find solutions in order to create customer confidence. As a consequence, Alternative Dispute Resolution mechanisms have been established and their use has considerably increased in the EU.

In the field of financial services and in particular payments, FIN-NET is regarded as an important tool for increasing confidence in cross-border trade and financial transactions. Currently, there is an obligation for Member States to ensure the existence of appropriate Alternative Dispute Resolution procedures in the field of cross-border credit transfers[50]. The bodies in the Member States operating Alternative Dispute Resolution procedures cooperate for cross-border disputes in the FIN-NET network.

During the consultation process, all parties have recognised that an extension of Alternative Dispute Resolution mechanisms to all payments – national and cross-border – could bring further benefits for the Single Payment Area. It would be in line with the philosophy of the Internal Market as a domestic market and equality of treatment between national and cross-border payments.

The setting-up and existence of Alternative Dispute Resolution mechanisms are without prejudice to the rights of the parties to use existing judicial procedures.

- ***Possible ways forward***

While considering the extension of Alternative Dispute Resolution mechanisms in the Internal Market to all categories of payments, national and cross-border, the following should be considered:

  – Adoption of binding principles for the functioning of Alternative Dispute Resolution bodies. The principles[51] proposed in Recommendation 98/257/EC[52] and adopted for FIN-NET could be used. They should ensure the proper functioning and independence of those schemes, which is crucial for their credibility.

---

49 See also Commission Green Paper on alternative dispute resolution in civil and commercial law (COM/2002/196 final).

50 Under Directive 97/5/EC, Article 10.

51 These are: independence, transparency, adversarial principle, effectiveness, legality, liberty, representation.

52 JO L 115, 17/04/1998, p.31-34.

– As in Directive 97/5/EC, the practical establishment (public, private, etc.) of Alternative Dispute Resolution bodies at national level should be left to the Member States and built on existing schemes.

One option could be to extend the current provisions of the Cross-Border Credit Transfer Directive (Article 10) to all kinds of payments. The draft Article on Alternative Dispute Resolution could read as follows:

Article on Alternative Dispute Resolution

"Member States shall ensure that there are adequate and effective out of court complaints and redress procedures in compliance with Recommendation 98/257/EC for the settlement of disputes between a payment service user and his payment service provider, using existing bodies where appropriate".

The Commission services invite views on this approach.

Annex 10: REVOCABILITY OF A PAYMENT ORDER

- ***What is the issue / problem?***

Revocability means the possibility for the originator of a payment order to lawfully cancel it. This definition does not cover the right of a payer to reject a debit from his account *based on a direct debit transaction*, since the execution of the payment is, generally, initiated by the beneficiary and not by an order of the originator[53].

So far, only the provisions of the Settlement Finality Directive[54] exist at EU level, providing for rules on the irrevocability of payments processed through notified systems. European legislation on revocability with regard to the rights of Payment Service User and Payment Service Provider, however, does not exist.

This lack of harmonised legislation leads to diverging rules within the EU[55]:

- With regard to credit transfers, some MS have legislation which includes a right to revoke a payment order up until the time of execution, other MS's legislation extends until the amount to transfer has been credited to the beneficiary's account, while others still leave this right to contractual agreements between the parties involved.

- For card payments, the situation is also fragmented: some MS do not have any binding legislation, others prescribe that any card payment is irrevocable, and others allow for the possibility to revoke a card payment only under specific circumstances (e.g. revocability of a card payment, if the payment order and the card number has been given, but without presenting the card itself as e.g. in e-commerce).

Diverging national rules determining the revocability of payment orders within the EU an obstacle to the well-functioning of the Internal Market. It may also degrade the legal certainty about the finality of payments. Such a situation may impair the proper functioning of payment systems in the Internal Market. It may also confuse market participants and in particular the Payment Service User.

- ***Possible Ways forward***

Harmonised revocability rules could improve the efficiency of existing and forthcoming payment systems, notably if the finality of payments intervenes at as early a stage as appropriate[56]. This would also provide more transparency for Payment Service Users.

Alternatively, one might consider that it is sufficient to leave the issue to self-regulation by Payment Service Providers, while only imposing specific harmonised legal information

---

53 Therefore, the right to reject a debit on the payer's account will be discussed in the context of direct debit in general, see Annex 16.

54 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, OJ L166 of 11.06.1998, p. 45.

55 Information about existing national legislation can be found in the table "National rules related to the right to revoke a payment (MARKT/4010/2003 - Final Draft)" – http://europa.eu.int/comm/internal_market/payments/.

56 The need for and feasibility of specific revocability rules for payments related to e-commerce in order to improve the consumer's rights when buying via the internet goods or services to be paid in advance will be discussed in Annex 11.

requirements with regard to the applicable revocability rules. Self-regulation, however, could not contradict existing binding national legislation. Self-regulation which would achieve a harmonised revocability-regime within the Internal Market is therefore rather unlikely. EU legislation seems therefore to be a preferable approach.

The forthcoming New Legal Framework for Payments could provide for harmonised revocability rules in order to improve transparency and to ensure legal certainty by determining the event / fact when a payment order becomes irrevocable, irrespective of whether payments are processed through notified systems or not. Those rules may have to distinguish between different possible means of payments.

The main difference between different kinds of payment instrument is that the payment order is either directly given to the originator's Payment Service Provider or that it is given via the beneficiary. Examples are a credit transfer order (first case) and a card payment order (second case). In the first case, the trust and confidence of the beneficiary in the finality of a payment arises when the payment has been credited to his account, whereas in the second case the beneficiary can already trust in a *forthcoming* execution of the payment order, which he has accepted instead of a payment.

Such rules could apply to every kind of payment based on an originator’s order, i.e. to "classical" means of payments (credit transfers, card payments) as well as to modern or new forthcoming payments (e.g. internet or mobile payments). Legal certainty would therefore be independent from technical developments and innovations and alleviate a major concern against “un-flexible” legal provisions.

In case of a harmonised regime, the forthcoming legal provisions could be read as follows:

Article for payment orders given directly to the payment service provider (e.g. credit transfer)

"A payment order given by the originator to his payment service provider is revocable, [until the originator's account has been debited] ***or*** *[until the money transfer has been initiated] or [until the payment order has been executed] or [until the amount to transfer has been credited to the beneficiary's account]."*

By providing four alternatives at this stage, the Commission invites all interested parties to comment on the most appropriate wording from a technical and practical point of view. The provision should ensure legal certainty.

A fifth option could be to provide for irrevocability of the order right after the order has been given to the Payment Service Provider. This, however, would hinder an originator from also revoking a payment order to be executed at a later date. Prohibiting the right to revoke such a payment order, as long as nobody has worked on the execution, would be excessively strict.

Article for payment orders given via the beneficiary (e.g. card payments)

"A payment order given by the originator via the beneficiary of the payment is irrevocable[, except if the amount was not determined when the order was given]."

This provision would, generally, take into account the need of a beneficiary to trust in the validity and finality of a given payment order As the payment order is accepted instead of a cash payment, it has to be as "secure" as cash. Otherwise non-cash means of payment might never replace cash payments.

However, there might be a need for a specific right to revoke a payment order, if the amount was not determined by the originator when the order was given (e.g. as a payment guarantee preceding a final payment for car rental, rapid hotel check-out procedures etc.). This was also provided for in Article 5 of the Recommendation 97/489/EC.

Rules on irrevocability would not impede any other legal or contractual rights of the Payment Service User, such as refund relating to the legal right of withdrawal (e.g. cooling off period) or a refund resulting from a breach of contract by a merchant. They are also without prejudice to the Payment Service User's rights in the case of unauthorised transactions, where the payment order is simply not valid. A refund is a legally independent transaction between the contractual parties and separate to the payment order. These legal rules should promote the efficiency of payments and payment systems as well as sufficient consumer protection. The Commission services welcome views on this approach and the effects on these objectives. Comment are, in particular, also requested on the exception of the rule of irrevocability in the case of a payment order in which the amount was not determined.

Annex 11: THE ROLE OF THE PAYMENT SERVICE PROVIDER IN THE CASE OF A CUSTOMER / MERCHANT – DISPUTE IN DISTANCE COMMERCE

- ***What is the issue / problem?***

The March 2001 Communication[57] from the Commission on e-commerce and financial services recognises that there is a "lack of coherent legislative basis to support refund in the internal market" and that this situation "inhibits chargeback from operating, particularly in respect of cross-border transactions".

The question to be addressed is whether and to what extent a Payment Service Provider should have a role in a commercial transaction between two contractual parties, the consumer and the merchant. Of special interest are situations where the product or service is paid in advance and is not delivered by the merchant (e.g. consumer complaint "I did not get it"). Payments in advance are presently more frequently asked for in distance selling mode than in face to face.

In the case of problems with the product, it is generally easier for a consumer to use his right of withdrawal, where this exists, or to seek redress in the case of face-to-face purchases. However, if problems arise in distance selling, consumers may be less easily able to get into contact with the merchant, since he may be located far away etc. In spite of the many initiatives to increase consumer confidence and protection for distance commerce in the EU[58], trust of consumers in non-face-to-face commerce is in many situations difficult to achieve. It is, therefore, worth considering what could be done to facilitate consumer redress in such cases. Introducing products that provide comparable levels of protection across the EU would help to overcome consumer concerns regarding cross-border transactions in general and e-commerce in particular. Since distance commerce is also very much linked with the use of remote payment means and payments are almost always done by non-cash means of payments, the Payment Service Provider plays a crucial part. However, no specific Community legislation exists on the Payment Service Provider's role in the case of contractual disputes between the consumer and the merchant in distance commerce.

---

57 COM(2001)66 – Communication from the Commission to the Council and the European Parliament on E-commerce and financial services.

58 The relationship between the consumer and the merchant in the case of non-face-to-face commerce is regulated in the Distance Selling Directive (97/7/EC). The Directive lays downs the main rules applicable to distance contracts including the rights of withdrawal for goods and services concluded between a supplier and a consumer. As regards financial services, the Distance Marketing Directive (2002/65/EC) provides similar protection.

- ***Possible ways forward***

Consumer's trust in e-commerce could be improved if the Payment Service Provider's responsibility in case of merchant / customer – disputes is strengthened. However, whether and especially how this could be achieved is very controversial.

So far, mainly two ideas have been discussed during the preliminary consultation period on the forthcoming Legal Framework for payments:

(1) the establishment of some sort of joint liability between the Payment Service Provider and the merchant in case of non-delivery of a product (or even further in case of non-conformity of a delivered product);

(2) specific revocability rules for payments made in e-commerce, e.g. by providing that remote payments in the case of distance selling contracts are revocable until the merchant provides evidence to the Payment Service Provider that he has delivered.

Results of earlier consultations have illustrated that consumer organisations are in principle in favour of the discussed approaches, in particular of the possibility to seek reimbursement through the Payment Service Provider. On the other hand, the payment industry raised, in particular, strong reservations about the feasibility of this approach and about the increased costs for the consumers. In their view there should be a clear distinction between the purchase contract, on the one hand, and the execution of the payment, on the other.

At present, the level of consumer protection in e-commerce varies from one product to another and from one Member State to another:

- In the United Kingdom, Finland and Sweden refund is a legal requirement for credit cards.
- Some payment card companies offer specific payment products which provide for contractual liability or other refund possibilities through the Payment Service Provider, sometimes at a higher price
- Some internet-platforms offer to handle the payment process by ensuring the delivery of the product
- Some companies offer the possibility to do the payment at the moment when the (physical) goods are delivered (e.g. by making the payment via the delivery service).

Several systems or provisions already exist – such as those mentioned above – and more are being developed. However, if these solutions appeared to not live up to the expectations of distance commerce users, Community actions for all commercial transactions in distance commerce (e- and m-commerce) aimed at addressing this issue at EU level might be a possible, by mandatory rules, self-regulation or a combination thereof.

Any future solutions should provide consumer protection at a reasonable price. A balanced approach requires taking account of three guiding principles:

(1) Any solution needs to be easily understandable and convenient for consumers.

(2) The principle of neutrality between payment instruments used in distance commerce.

(3) Any solution should be proportionate to the problem and should not introduce unreasonable costs on the payment service.

The Commission invites all interested parties to comment on the above issues, particularly with regard to their effects on consumer protection and on payment market efficiency. Also additional proposals to overcome perceived problems in order to enhance consumer confidence and to foster distance commerce, are welcome.

ANNEX 12: NON-EXECUTION OR DEFECTIVE EXECUTION

- ***What is the issue/problem?***

As a general principle, a Payment Service Provider should be responsible for executing a payment order according to the mandate given by the Payment Service User. If a Payment Service Provider does not fulfil its obligations towards a Payment Service User, the question of liability arises.

Harmonised rules covering the obligations and liabilities of the concerned parties in the case of non- or defective execution would facilitate the establishment of a level-playing field between the Payment Service Providers in the Internal Market. It would also guarantee a uniform high level of consumer protection. The aim should be that a Payment Service User has the same level of protection wherever s/he buys or uses a payment service in the Internal Market.

The extent and the nature of the liability in the case of non-execution, where the payment has not arrived on the beneficiary account, or defective execution, where the full amount has not arrived or the payment has arrived later than agreed or foreseen in law, need to be addressed.

In this context, it is important to decide whether a general rule could be applied to all kinds of payment services, such as credit transfers, card payments etc., or whether the specific nature of a certain payment instrument would require a special treatment.

Presently no comprehensive legal framework exists for all payment instruments:

- Directive 97/5/EC includes a provision of strict liability (the so-called "money-back guarantee") of the Payment Service Provider to refund a cross-border credit transfer up to a specified amount, if it does not arrive at the beneficiary's account or arrives later than agreed (see Art. 6 and 8).

- As regards electronic payment instruments, Recommendation 97/489/EC stipulates that the issuer should be liable for the non-execution or defective execution of a holder´s transaction (see Art. 8). In addition, the Recommendation stipulates that the issuer should have the burden of proof that the transaction was accurately recorded and entered into the accounts (see Art. 7).

- ***Possible ways forward***

There seems to be a general understanding that a Payment Service Provider should be responsible for the accurate execution of a payment order and have the burden of proof that the transaction was accurately recorded, executed and entered into the accounts. The Commission considers a strict liability rule for the Payment Service Provider as an appropriate way forward in this context, as the Payment Service User may not influence any third party contractual relationships that the Payment Service Provider may have with other parties in the payment process. Strict liability saves the Payment Service User from having to contact a number of Payment Service Providers in the payment chain in order to establish whose fault it was, a procedure for which the Payment Service Provider is much better equipped than the Payment Service User. The question of consequential damage has not been raised as such in this context as there was very little support during the pre-consultation on this issue.

One general rule applicable to all payment instruments would be preferable, as this would guarantee the same level of protection for the Payment Service User and thereby facilitate customer choice between different payment services and as well as a level-of-playing field between the Payment Service Providers. This approach would mean that there would no longer be a need for a separate provision, such as the so-called money-back guarantee for credit transfers. In addition, as the existing money-back rule covers only cross-border credit transfers, it would be justified to change it anyway as the scope of the new legal act will cover all payments ("national" and "cross-border) in the Internal Market.

Draft legal provisions could read as follows:

"1. The Payment Service Provider shall be liable for the non-execution or defective execution of a payment order, which the Payment Service User has initiated in accordance with his obligations [mandatory / contractual].

2. Paragraph 1 shall be applicable even if a payment order is initiated at devices/terminals or through equipment which are not under the Payment Service Provider's direct or exclusive control, provided that the order is not initiated at devices/terminals or through equipment unauthorised for use by the Payment Service Provider.

3. Without prejudice to paragraph 4, liability under paragraph 1 shall include the amount of the non-executed payment order, as well as charges and interest thereon, if any;

4. Further financial compensation shall de determined in accordance with the law applicable to the contract concluded between the Payment Service Provider and Payment Service User.

5. If the Payment Service User claims that a payment order has not been accurately executed, the Payment Service Provider shall prove, without prejudice to evidence to the contrary produced by the Payment Service User, that the payment order was accurately recorded, executed, and entered into the accounts."

In order not to place an unreasonable burden on the Payment Service Providers relating to circumstances which are objectively out of their control, there may be a need to introduce a provision relating to "*force majeure*". The precise formulation of such a provision needs to be considered.

In addition, to secure the same level of protection for the Payment Service User a provision relating to the mandatory nature of these provisions may be needed. These provisions could read as follows:

"1. The Payment Service Provider may not contractually exclude or limit his obligations and liabilities under this legal act."

The Commission services welcome views on this approach and its impacts.

ANNEX 13: OBLIGATIONS AND LIABILITIES OF THE CONTRACTUAL PARTIES RELATED TO UNAUTHORISED TRANSACTIONS

- ***What is the issue/problem?***

As electronic payments, such as card payments and internet banking, are becoming increasingly important payment instruments in the Internal Market, the question of fraudulent usage of a payment instrument is also becoming even more important. In the case of fraudulent use of a payment instrument[59], the legal safeguards for the concerned parties have to be in place in the Internal Market. These legal safeguards should provide both a high level of consumer protection and the efficiency and security of the Single Payment Area, while respecting the need of fraud prevention. The user of payment services should have the same high level of protection where-ever they buy or use their payment services in the Internal Market.

Presently, no comprehensive legislation exists at EU-level on the issue of unauthorised transactions: Recommendation 97/489/EC regulates the relationship between the issuer and the holder of electronic payment instruments in this respect. Directive 97/7/EC and Directive 2002/65/EC regulate the case of fraudulent use of a card payment in distance commerce.

- ***Possible ways forward***

The Commission services consider that the Recommendation 97/489/EC provides a good basis for addressing the relevant obligations and liabilities of the contractual parties in the case of unauthorised transactions.

In this respect a fair balance between the liabilities and obligations of the Payment Service Provider and Payment Service User may be achieved taking account of the general objectives mentioned above. In this respect one has to consider the effects the legal provisions may have on the incentives of the contractual parties. For instance, legislation should not through distorted incentives increase the likelihood of fraudulent behaviour of the legitimate Payment Service User i.e. so-called first-party fraud.

It is also important to analyse whether a general rule may be applicable to all kind of payment instruments, such as internet banking, card payments etc., or whether the specific nature of a payment instrument justifies a special treatment in this context. From the outset the Commission services consider that one set of general rules could be applicable to all non-cash payment services.

Draft legal provisions could read as follows:

Article on the obligations of the contractual parties

1. The Payment Service User shall

(a) use the payment instrument in accordance with the terms governing the issuing and use of the instrument; in particular the Payment Service User shall take all reasonable steps to keep

[59] A payment instrument shall be understood in this context to cover also the personal identification means or other secret code enabling a payment execution/order.

the safe the payment instrument and any means, such as a personal identification number or other code, which enables it to be used;

(b) notify the Payment Service Provider (or the entity specified by the latter) without delay after becoming aware of:

- loss, theft or misappropriation of the payment instrument and/or the means of identification which enable it to be used

-the recording on his account of any unauthorised transactions any error or other irregularity in the maintaining of his account

2. The Payment Service Provider shall

(a) not disclose a Payment Service Users personal identification number or other code, except to the Payment Service User

(b) not dispatch an unsolicited payment instrument, except where it is a replacement for a payment instrument already held by the Payment Service User

(c) keep for a sufficient period of time, internal records to enable the transactions to be traced and errors to be rectified

d) ensure that appropriate means are available to enable the Payment Service User to make the notification required under paragraph 1. Where notification is made at a distance, the Payment Service Provider (or the entity specified by the latter) shall provide the Payment Service User with the means of proof that he has made such a notification.

3. If the Payment Service User claims that a transaction was not authorized, the Payment Service Provider shall provide evidence that the transaction was authorized, accurately recorded, entered into accounts and not affected by technical breakdown or another deficiency.

4. The elements of evidence referred to in paragraph 3 shall be without prejudice to evidence to the contrary produced by the Payment Service User. In particular, the use of a payment instrument or any personal code which enables it to be used shall not, by itself, be sufficient to entail that the payment was authorised by the Payment Service User, if the Payment Service User provides factual information or elements, which would allow the presumption that he could not have authorised the payment.

Article on liabilities between the contractual parties

1. The Payment Service Provider shall be liable for transactions executed without the Payment Service User's authorisation.

2. The Payment Service Provider shall not be liable if the Payment Service User acted with gross negligence or fraudulently. In determining the Payment Service User's gross negligence, account shall be taken of all factual circumstances.

3. When liable, the Payment Service Provider shall refund without delay to the Payment Service User the sum required to restore the payment account to the position it was in before the unauthorized transaction took place.

4. Further financial compensation shall be determined in accordance with the law applicable to the contract concluded between the Payment Service Provider and the Payment Service User.

5. The Payment Service User shall bear the financial consequences resulting from the loss, theft or misappropriation of the payment instrument, which may not exceed 150 euros, if s/he has not fulfilled s/he obligation to notify the Payment Service Provider as required.

6. After the Payment Service User has notified the Payment Service Provider as referred to in Article [XXX], s/he shall not be liable for the financial consequences of the loss, theft or misappropriation of the payment instrument, except where he/she acted fraudulently.

7. The limit referred to in paragraph 5 shall not apply if the Payment Service User acted with gross negligence or fraudulently.

8. If the Payment Service Provider did not fulfil the obligation to provide adequate means for the notification of lost/stolen/misappropriated instruments as referred to in Article [XXX], the Payment Service User shall not be liable for the financial consequences resulting from the loss, theft or misappropriation of the payment instrument, except where he/she acted fraudulently.

The Commission services welcome views on this approach and views on the effects on customer protection and payment market efficiency are especially sought.

Annex 14: THE USE OF "OUR", "BEN", "SHARE"

- ***What is the issue/problem?***

Terminology is used in the payment sector, OUR (all charges to the originator of a payment), BEN (all charges to the beneficiary) and SHARE (shared costs between originator and beneficiary), which refers to the manner of sharing of costs between the originator and the beneficiary for the execution of credit transfers. This terminology has been used colloquially in the context of the Directive 97/5/EC on Cross-Border Credit Transfers, even though it does not appear in the text itself. The Directive foresees all three options for the sharing of charges between the originator and the beneficiary, of which OUR is the default option. The setting of OUR as the default intended to avoid double charging and to ensure the arrival of the full amount transferred on the account of the beneficiary.

Under Regulation 2560/2001/EC on Cross-Border Payments in Euro[60], the charges for cross-border credit transfers will have to be the same from 01.07.2003 as those for national transfers. Consequently, there should be no need for a default option as regards cross-border payments covered by the Regulation. A provision stating that the payment should be executed for the full amount should be sufficient in order to avoid any deductions in the payment chain.

However, due consideration should be given to those credit transfers that are not covered by the Regulation, which can be divided into 2 categories:

- non-euro or non-krona payments and
- payments in the range of over 12.500 euro and up to 50.000 euro between 01.07.2003 and 01.01.2006.

As to the first category, it should be considered whether a provision stating that the payment should be executed for the full amount (see legal proposal at the end of this Annex) would be sufficient in order to avoid any deductions in the payment chain or whether Directive 97/5/EC should remain unchanged in this respect. The first alternative would result in a major simplification of legislation.

As regards the second category, the same question could be raised. According to Article 3 of the Regulation on cross-border payments, the principle of equality of charges between national and cross-border payments will apply to credit transfers up to 12.500 euro from 01.07.2003, and only after 01.01.2006 to credit transfers up to 50.000 euro. Another possibility could be to extend the scope of the Regulation to cross-border payments between 12.500 euro and 50.000 euro between 01.07.2003 and 01.01.2006.

[60] Also applicable to the Swedish krona, according to a decision by the Swedish Authorities (OJC 165/36, 11.07.2002).

- ***Possible ways forward***

As explained above, specific rules applicable to cross-border credit transfers in respect of the sharing of charges between the originator and the beneficiary can possibly only be justified for those credit transfers which are not covered by the Regulation. In that case, the corresponding provisions of the Cross-Border Credit Transfers Directive (Article 7, "obligation to execute the cross-border transfer in accordance with instructions") should only remain applicable to payments that are not covered by the Regulation and contractual freedom should apply for payments covered by the Regulation.

In addition, as this "full amount" principle is largely used at national level and meets with overall broad support[61], it should be established in the New Legal Framework for Payments that the full amount transferred by the originator should be credited to the beneficiary's account. This principle should be extended to all payments. A draft legal proposal could read:

Article on the obligation to execute a payment for the full amount

"The full amount specified in a payment order shall be credited without any deduction to the beneficiary, without prejudice to explicit agreements between the beneficiary and his payment service provider".

The Commission services welcome views on the above mentioned approach and its impacts.

[61] It is the principle established in the "CREDEURO" concept of the European Payment Council.

Annex 15: EXECUTION TIMES FOR CREDIT TRANSFERS

- ***What is the issue / problem?***

The existing Cross-Border Credit Transfers Directive deals with the time limit for executing a cross-border credit transfer: unless otherwise agreed between the Payment Service User and his Payment Service Provider, a cross-border credit transfer should by default be credited at the account of the beneficiary's Payment Service Provider within 5 working days. Likewise, the beneficiary's Payment Service Provider has to credit the beneficiary's account within one working day after having received the credit transfer, unless the beneficiary and his Payment Service Provider agreed on different execution times. The Directive thus provides for a default execution time for cross-border credit transfers of 5+1 days.

As already announced by Commissioner Bolkestein before the European Parliament in 2000, the Commission intends to propose shortening the default maximum execution time from the current 6 working days to a much shorter period. Modern technology and recent developments should allow for such reduced delays for cross-border credit transfers. A recent Commission study showed average execution times of 2.97 days, an average which is well below the obligations laid down by the Directive. 95.4% of the transfers arrived within the default time specified in the Directive, i.e. within six working days. 99.7% of the transfers arrived within 15 days. The introduction of the euro as a single currency contributes to more expedient execution.

However, as the new legal instrument will deal with all payments in the Internal Market in order to facilitate the establishment of a Single Payment Area, a rule applicable only to so-called "cross-border" credit transfers may not be the appropriate way forward in this context. There should be no major differences between "cross-border" payments and "national" payments in the Internal Market. Any legal measures should be destined to further develop the Internal Market for retail payments and to align conditions of "national" and "cross-border" payments.

- ***Possible ways forward***

The Commission services consider an approach which does not discriminate between credit transfers executed in the Internal Market as the right way forward. Many respondents to the pre-consultation considered, self-regulation was the right way forward in this context. However, the Commission has considerable concerns that legal certainty and transparency relating to the execution of credit transfers may not be achieved through self-regulation. Therefore legal provisions applicable to all credit transfers in the Internal Market may be needed in order to guarantee legal certainty to all parties involved – notably the Payment Service Users.

The only exception could be non-euro "cross-border" credit transfers, which may require a separate approach, as these may not be technically ready to be put on the same level of equivalence with credit transfers executed in euro. In this case, the existing rules of the Directive could be grandfathered.

A draft legal provision could read as follows:

Article on execution time

"After acceptance of a credit transfer order it shall be executed within the time limit agreed with the originator, or in the absence of such a time limit, at the latest at the end of the third [banking business / working] day following the date of acceptance of the credit transfer order [payment order]."

The Commission services welcome views on the above mentioned approach and its impacts in terms of customer protection and payment market efficiency.

Annex 16: DIRECT DEBITING

- ***What is the issue / problem?***

The characteristic of a direct debiting system is that the authorized beneficiary initiates the transfer of funds from the account of the customer to his own account. Direct debiting techniques are mostly used for recurring payments in the context of public utility (electricity, telephone etc.), insurance or reimbursements billing. Generally, this payment method is based on contractual terms and the payer has mandated his bank or the beneficiary to debit his account.

Direct debiting is frequently used within several countries but is so far nearly non-existent on a cross-border basis. This results from legal differences between existing national direct debit schemes on the one hand, and from a lack of technical interoperability between the national schemes on the other.

As the direct debit technique is already used on a national basis as an increasingly convenient and effective payment method, it should be extended to the whole Internal Market. However, an extension will only be successful and accepted by market participants if, beyond any technical developments, the rights of the Payment Service Users are sufficiently taken into account. The concerns of the payer in case of unjustified or unauthorised debits have especially to be addressed. If the debtor does not have the possibility to reject a debit from his account, or if the time to reject a debit is not long enough, he will not use the direct debiting method.

So far, national systems differ quite significantly from each other. Differences can exist with regard to the procedure of mandating the beneficiary by the debtor to initiate the payment process, or with regard to the obligations of the involved Payment Service Provider to ensure that a direct debit is based on an existing and valid mandate, or with regard to the payer's right to reject a direct debit.

The development of a future European direct debit scheme will have to ensure that crucial elements do not impair interoperability. In addition, it needs to be based on a set of rules which can ensure the confidence and trust of both Payment Service Users and Payment Service Providers, as well as efficiency in order to overcome concerns to cross-border direct debit transactions arising out of differences in national behaviour.

- ***Possible Ways forward***

The European Commission and the European Payment Council are working very closely together on this issue in order to ensure that a direct debit will be able to be realised in the near future within an efficient and well-functioning European payment infrastructure. Work on this project is still ongoing. The European Payment Council is currently developing a business model for a possible Pan-European direct debit scheme, which will allow direct debit transactions in euro within the Internal Market.

At the same time, the European Commission is undertaking a study on existing national direct debit schemes in order to find out which specific legal aspects will have to be addressed in order to remove legal barriers and to build up trust and confidence in the forthcoming system. The results of the study, combined with the input of the European Payment Council's work, will be the basis for the forthcoming New Legal Framework.

The New Legal Framework will address the crucial legal obstacles which hinder efficient cross-border direct debit payments. This will include the request of Payment Service Users for sufficient protection, such as the right to reject a debit.

Forthcoming provisions will harmonise existing differences as far as they constitute obstacles to cross-border direct debiting, in order to create trust and ensuring legal certainty of market participants. The most important point is the initial authorisation given by the debtor allowing the creditor to initiate direct debit.

However, any legislative proposal should not impair existing and well-functioning national schemes. On the other hand, one aim of the legal framework is to establish rules, which should – as far as is possible and useful – cover all payment services irrespective of whether they are purely national or Pan-European.

Contributions on the necessary legal requirements for direct debit schemes would be helpful for future decisions.

ANNEX 17: REMOVING BARRIERS TO PROFESSIONAL CASH CIRCULATION

- ***What is the issue/problem?***

All euro zone countries share the same currency, but some difficulties remain for the cross-border transport of cash.

An important obstacle to the transportation of cash on a cross-border basis are the rules which apply to the professional activity of money transport. As the relevant rules relating to the transport of cash vary widely among the euro zone countries and since they have not yet been harmonised, such transportation is virtually impossible to operate cross-border. A bank cannot deliver or receive cash from retailers on the other side of the border in another Member State.

- ***Possible ways forward***

The Commission has created a working group with the cash transport industry to analyse solutions for Cash-In-Transport activities An Internal Market approach needs to be implemented which, at the same time, shall increase the efficiency of that activity and reduce the cost.

The Commission services invite the market to raise any additional problem in this context and to suggest possible solutions relating to the wholesale cash market.

Annex 18: DATA PROTECTION ISSUES

- ***What is the issue/problem?***

The exchange of information among parties concerned is an essential element in any effective fraud prevention strategy. The investigation and prosecution of payment fraud cases presuppose such an exchange between financial institutions and law enforcement agencies both within each EU Member State and at cross-border level. Efficient information exchange also takes place in all EU Member States within the private sector (mostly within the payment industry) for preventative purposes[62]

The rules for handling personal data in the EU are laid down in Directive 95/46/EC on data protection[63]. This Directive 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 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.

The above conditions for the collection and processing of personal data also apply to the exchange of information between operators in the payment markets and between these and the authorities involved. Article 13, letter d) of the Directive offered Member States the possibility to derogate from these requirements, if necessary, in order to prevent, investigate, detect, and prosecute criminal offences. However, not all Member States have implemented this derogation or have implemented it with the same scope. The result is that the collection and processing of some personal information to prevent payment fraud is allowed in one Member State and prohibited in another.

The uneven implementation of the Directive in the Member States may create problems for systems which rely on data to be collected in, and exchanged with, other Member States. The Commission consider that it is necessary to further approximate rules on the exchange of information taking place within each country and among EU Member States in order to prevent fraud.

The Commission services had meetings with representatives of the private sector in order to identify actual problems. The main issue seems to be that, to prevent fraud, the payment card business operates centralized or local fraud prevention databases which provide information on high-risk and fraudulent merchants. Those databases rely on input received from the banks which maintain contractual relationships with merchants (acquirers). The purpose of the data collection is to enable acquirers to make an informed decision when entering into an agreement with merchants whose contracts have been terminated due to breach, collusion or excessive fraud. Since the implementation of the Directive into national legislation, acquirers in certain Member States have been reluctant to report fraudulent merchants in these databases, as they are concerned that such reporting would be contrary to their national data protection laws. Industry representatives expressed the view that these databases are

---

62 On-line "flagging systems" 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 sometimes taken in the retail sector, where incidents databases have been created

63 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ no. L 281 of 23 November 1995.

becoming outdated and incomplete, that they no longer can be relied upon and that this has resulted in a noticeable increase in fraud in the markets concerned. In turn, this increase in fraud has an impact on the cost of payment products and affects consumer trust.

At the recent EU Card Fraud Forum organised by the Commission in March 2003, law enforcement and public prosecutors requested greater clarification of existing EU data protection legislation in order to allow a wider cross-border exchange of information.

According to contributions received from the banking sector in the preparation of the present Communication, the excessive fragmentation of the current legal framework on data protection in the European Union is clearly perceived as an obstacle to the proper functioning of the Internal Market. The EU banking sector requested the EU legislator to adjust, where necessary, the data protection legislation in order to allow the sharing of fraud-related information between market participants.

- ***Possible ways forward***

The EU Fraud Prevention Action Plan[64] calls for an improved information exchange without prejudice to the rights and freedoms of individuals. It invites the Commission to examine the extent to which the uneven implementation of the Directive 95/46/EC has an impact on the fight against fraud and counterfeiting and to provide, in co-operation with national data protection authorities, guidelines on conditions for exchange of information related to fraud prevention.

To achieve clear and common rules, a first option would then be to prepare guidelines balancing the interests of the prevention of fraud with the respect of the fundamental rights and freedoms of individuals. These guidelines would facilitate common understanding and application of the data protection legislation with respect to fraud prevention activities. The Data Protection Article 29 Working Party[65] already established a mixed informal Working Group (representatives of the payment industry and of Data Protection authorities) to work on the guidelines. Data Protection Authorities in the Member States expressed willingness to establish guidelines, but needed more information from the private sector before having detailed legal discussions. This option, although desirable and useful, presents some limitations and might not be sufficient to achieve the intended outcome. Even if they are willing to agree on a common interpretation, the national data protection authorities are bound to respect the provisions of their national legislation and cannot derogate from them by way of interpretation. Accordingly, the first Report on the implementation of the Data Protection Directive ("the Report"), confirms that discussions in the Article 29 Working Party may enable issues affecting several Member States to be tackled on a multilateral basis, but that such discussions cannot lead to a *de facto* amendment of the Directive.

---

64 Communication from the Commission "Preventing fraud and counterfeiting of non-cash means of payment", COM (2001) 11 final of 9 February 2001, available at: http://europa.eu.int/comm/internal_market/payments/. The Action Plan aims at fostering a global and coherent approach to fraud prevention and is based on cooperation among all interested parties.

65 This group is composed by the Data Protection Commissioners of the EU Member States or their representatives. It meets periodically in Brussels and its secretariat is handled by the Commission services. The mandate of the Working Party includes *inter alia* the examination of questions covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of these measures and advice to the Commission on any proposed amendment of the Directive. The Working Party issues Opinions and Recommendations.

A second option could be to invite Member States to amend the relevant national rules with the view of achieving an identical legal framework in the EU which would allow a wider exchange of information for fraud prevention purposes. The Report acknowledges that there is considerable scope for improvement in the implementation of the Directive and confirms that the Commission's attention will continue to be focused on areas where divergent interpretations and/or practices are causing difficulties in the Internal Market. The work programme for a better implementation of the Directive foresees discussions with the Member States in 2003 and 2004. While the discussions are envisaged mainly for cases of incorrect transposition, the Commission, with the support of the national Data Protection authorities, may urge the Member States to introduce amendments to their legislation in order to provide harmonised rules in this area. The question is how to achieve this result in practice.

A third option could be a revision of Directive 95/46/EC. This possibility seems quite remote at the present time, especially as the late implementation by some Member States has meant that the Directive has not yet had the chance to work properly. Following discussions with the Member States, the Commission in its Report considered that a modification of the Directive was neither necessary nor desirable at present. This view seems to be shared by a comfortable majority of Member States and of national supervisory authorities. Having said that, the Commission will closely monitor the results of the work programme for a better implementation of the Directive and make proposals for further follow-up in 2005. Particular attention will be paid to full harmonisation to the facultative exceptions foreseen in Article 13 d) of the existing Data Protection Directive (a derogation from the requirements of the Directive in order to prevent, investigate, detect and prosecute criminal offices) and making them mandatory for all Member States.

A fourth option could be to include a provision corresponding to Article 13, letter d) of the existing Data Protection Directive in the New Legal Framework for Payments in the Internal Market. This provision could provide harmonisation on necessary derogations to data protection principles and compensate for the lack implementation of this option by some Member States. In the Report, the Commission states that Member States and supervisory authorities are expected to make all reasonable efforts to create an environment in which data controllers (especially those operating on a pan-European and/or international level) can conform to their obligations in a less complex and burdensome way and to avoid imposing requirements that could be dropped without any detrimental effects.

The Commission services invite all interested parties to indicate, in a detailed manner, the concrete problems notably regarding existing or non-existing Community legislation in this respect.

Annex 19: DIGITAL SIGNATURES

- ***What is the issue/problem?***

Digital certificates are used to identify parties (for example over the Internet) and enable secure, confidential communication between them. Identification and authentication of the parties and the integrity of messages are crucial in establishing secure payments, especially for on-line transactions.

While several electronic signature initiatives based on the concept of Public Key Infrastructure (PKI) are starting to be used for specialised purposes where a high level of security is required (e-government, notarisation of documents etc), in the field of e-commerce and m-commerce no PKI-based application is successfully deployed on a large scale in the business-to-customer environment. This lack of implementation may be due to the high costs of PKI technology and to the low level of user-friendliness of such applications. However the question arises as to whether legislation adequately supports the market by addressing all legal and technical issues arising in the context of payments.

The Directive on Electronic Signatures[66] establishes the general legal framework for electronic signatures in the EU by ensuring their legal recognition and free circulation within the Internal Market. The Directive identifies minimum requirements for qualified certificates, certification service providers and secure signature creation and verification devices, but does not cover applications in specific sectors. The Directive covers both electronic signatures (basically all types of authentication methods) and "advanced electronic signatures" (AES), which meet certain requirements (basically corresponding to digital signatures based on asymmetric cryptography) and are based on a qualified certificate and secure signature creation devices. From a legal standpoint, it is sometimes unclear what this enhanced legal status of AES [Eliminate abbreviations] means in practice, as some national laws have attributed particular legal effects to AES[67]. Moreover, some national provisions allow digital signatures to be used only by natural persons and not by legal persons.

At technical level, the Directive does not specify the requirements for “advanced electronic signatures” and leaves their clarification to the Electronic Signature Committee (composed by representatives of Member States). However, the Directive also allows for national accreditation schemes (public or private), which may have diverging practices[68] to be introduced or maintained. A clearer definition of the technical requirements for AES in the area of payments is desirable. In this respect, the work of the industry’s European Electronic Signature Standardisation Initiative (EESSI) aimed at creating *de facto* standards is of utmost importance.

---

66 Directive 1999/93/EC of 13 December 1999. The deadline for implementation by Member States was 19 July 2001.

67 For instance, the Spanish law introduces a presumption of authenticity and integrity when a document is signed using an AES. In the area of payments, the different legal effects granted to basic electronic signatures and AES can be very relevant. If a customer repudiates a transaction, a basic e-signature can be admitted as evidence in court, but does not automatically prove the customer’s participation. Instead, an AES would provide evidence of the customer’s participation and certify that the document was not altered after the signature.

68 For example, some countries hold the view that the storage of the private key (a secure signature creation device) can be satisfied only by the use of hardware devices, such as smart cards.

- ***Possible ways forward***

In the area of digital signatures, the legal uncertainties related to the status of AES in some Member States and the issue of digital signatures placed by legal persons may be addressed when assessing the correct and complete implementation of the Directive. Under this standpoint, the existing legal framework might be considered as sufficient and there may be no immediate need for further provisions.

On the other hand, the limited experience available[69] seems to show that technical barriers exist in order to qualify an electronic signature as absolute proof of a customer's authorisation of a payment. Moreover, there are problems related to the lack of mutual recognition of electronic signatures which hinder their development and implementation. It is necessary to ensure that there are no barriers to the full deployment of electronic signatures in the Internal Market. Further harmonisation is desirable, as the national laws currently differ also regarding the level of security to be reached by the certification providers, which might result in technical incompatibility.

The Commission is due to submit a report on the implementation of the Directive by the end of 2003. To this end, a study on the implementation of the Directive in the Member States is being finalised. Taking into account that this Directive was implemented with some delay and that the study should provide a much better understanding of the issues at stake, it would appear premature to propose new measures before knowing the outcome of the report.

The Commission services invites, however, all interested parties to indicate, in a detailed manner, the concrete problems relating to payment services and the ways to improve the situation via EU legislation.

---

69 The EU Member States had to implement this Directive by July 2001. Some Member States have transposed it with considerable delay, so that little practical experience has been acquired in its implementation.

Annex 20: SECURITY OF THE NETWORKS

- ***What is the issue/problem?***

In recent years several high-profile security breaches have taken place at databases of e-commerce merchants, credit reference agencies and government databases, where access was gained to customers' personal data, including credit card numbers. These attacks have resulted in increased opportunities for payment fraud and forced the banking industry to cancel and re-issue thousands of payment cards. A further consequence is the intangible damage to the merchant's reputation and to the consumer perception on the security of the Internet and the use of payment instruments in this environment. This strongly undermines consumer confidence in e-commerce. The problem is further compounded by the fact that many intrusions are not reported to the police[70].

Hacking incidents continue to occur with disrupting effects. The most recent trend of hackers is to attack the databases of payment processors, i.e. intermediaries to which payment providers have outsourced the processing of data.

- ***Possible ways forward***

In this area, Governments have reacted strongly by amending national penal legislation to adequately cover the new category of cybercrimes. At international level, the Council of Europe adopted the Cybercrime Convention[71]. In the EU, the Commission proposed in April 2002 draft rules providing a common definition of certain cybercrimes (including hacking into databases) in the EU and common penalties for offences[72]. In the area of payment systems, EU legislation against fraud and counterfeiting of non-cash payments was adopted in May 2001[73]. Preventive measures, such as minimum security requirements for online merchants accepting payment cards, are being discussed under the Fraud Prevention Action Plan[74]. Recently, the Commission proposed a Regulation[75] setting up the European Network and Information Security Agency (EUNISA). The establishment of an Agency responsible for Network and Information Security in the EU aims to achieve closer European co-ordination in this area. The role and responsibility of the Agency in the field of payment operations carried out in open networks may be of relevance.

---

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

71 The Convention provides common rules and sanctions for actions against the confidentiality, integrity and availability of computer systems, networks and data. It has been open to ratification since October 2001 and has not yet entered into force.

72 Proposal for a Council Framework Decision on attacks against information systems, COM (2002) 173 final.

73 Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting on non-cash means of payment (OJ no. L 149 of 2.6.2001). *Inter alia*, it criminalises in all Member States the behaviour of intentionally performing a payment transaction by introducing, altering, deleting or suppressing computer data (in particular identification data) or interfering with the functioning of a computer programme or system. Member States should implement this legislation by June 2003.

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

75 Proposal for a Regulation Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency, COM(2003) 63 final of 11 February 2003.

The approach followed so far by regulators has mainly consisted of amending penal legislation in order to cover new types of criminal behaviour and to sanction them adequately. The harmonisation of penal legislation against cybercrime, both in the EU and beyond, and cooperation with other jurisdictions has been strongly welcomed by stakeholders. One could conclude that there is no need for further legal provisions on the security of the infrastructure in the payment area and that further initiatives may be left to self-regulation.

However, the security of the communications networks and information technology has become crucial for the security of payment instruments and systems. The growth of Internet penetration and the increased use of e-payments and e-banking call for high levels of security in order to protect systems, transactions and personal data against unauthorised access. These factors, coupled with the frequency and relevance of hacking incidents, may justify further legal provisions aimed at protecting personal data against unauthorised disclosure or access.

This principle is already enshrined in Article 17 of Directive 95/46/EC[76], which provide for the obligation of the person processing personal data (the controller) to take appropriate measures to protect them against, *inter alia*, unauthorised access. When a third party (processor) is involved, the controller must choose a processor providing sufficient guarantees in respect of the technical security and organisational measures governing the processing. The obligation to adequately protect personal data must be extended to the processor by contract or legal act. Due to the limited enforcement of the data protection legislation in this area, it is doubtful that this provision is currently implemented in a wide and strict way.

It would be also necessary to concretise the general obligations of result contained in this Article of the Data Protection Directive, for example with a view to:

- Ensure that payment service providers and merchants storing and/or processing, in a professional capacity, personal data related to payment transactions (eg name and address of the customer, credit card and bank account numbers) implement appropriate technical and organisational measures with respect to network security to prevent unauthorised access (i.e. hacking) to such data.

- Ensure that the customers are informed in case security breaches allow unauthorised access to such data by third parties through information networks.

- Ensure that the possible financial consequences resulting from the security breach (payment fraud, counterfeiting, other misuse of the data such as identity theft) are not met by the customer.

- Ensure that payment service providers and merchants outsourcing all or part of its operations to a third party perform checks on its security systems and organisational procedures with respect to network security.

In order to achieve these results, a first option would be to introduce in the New Legal Framework for payment additional provisions complementing those of existing EU legislation (both Article 17 of the Data Protection Directive and similar provisions in Directive

---

[76] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ no. L 281 of 23 November 1995. A similar provision is contained in Article 4 of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ no. L 201 of 31 July 2002.

2002/58/EC). This option present some benefits but also some problems such as the correct articulation with the existing legal framework both at Community and at national level.

A second option would be to refrain from further legislation and ensure that the European Network and Information Security Agency, once established, plays an important role in collecting data and providing expert advice to financial institutions and merchants on incidents related to payment operations carried out in open networks. This role might be extended to cover the possibility of concluding agreements with market participants on the security of their information systems, which may provide for financial penalties in case of breach.

The Commission services invite views on the importance of this issue. Especially views on the benefits legal measures in this context would provide.

Annex 21: BREAKDOWN OF A PAYMENT NETWORK

- ***What is the issue/problem?***

Both Payment Service Providers and users are affected by technical breakdowns in a payment network. Operational disruptions in the payments infrastructure (e.g. the temporary loss of telecommunications or computer processing ability) may create situations of risk where liability may arise. In the area of payment systems, risks are enhanced by two factors:

- Payment systems have network externalities. Therefore, the participating institutions, in addition to the safety of their own systems, are more vulnerable to system breakdowns happening in other institutions. Payment Service Providers have generally foreseen contingency measures and procedures to deal with these problems.

- Some Payment Service Providers tend to outsource data processing and other technology intensive activities to third parties.

In the case of breakdown of a payment network, users are unable to access their accounts, make payments and complete transactions. The question is whether there should be a liability of the Payment Service Providers toward the users in such situations.

The existing EU legal framework does not fully regulate this issue. When a valid payment order exists, there seems to be a general understanding that a Payment Service Provider should be responsible towards the customer for its accurate execution (see Annex 12). There is less clarity on the question as to whether the Payment Service Provider should also be liable:

- Towards a customer that could not issue a valid payment order because it was impossible to access his/her payment facilities (e.g. Internet banking website) and as a result sustained a financial damage (e.g. a penalty for delayed payment);

- Towards a merchant, for example in the case of card payments, when the payment card network is temporarily unavailable and the merchant loses potential profits due to the inability of his own customers to complete transactions by payment card.

- ***Possible ways forward***

The Commission at this stage has no final stance on the possible liability of a Payment Service Provider toward a customer or a merchant in case of breakdown of a payment network. In the case of a merchant, such liability may give rise to practical difficulties concerning the burden of proof and the determination of the amount to be refunded to the merchant. Namely, in the above example (merchant accepting payment cards with payment card network temporarily unavailable) it may be difficult for the merchant to prove how many customers (or simply that some customers) could not complete payment card transactions; it may be even more difficult to demonstrate that, as a result of the breakdown, the merchant had lost a specific amount in sales and profits (as the customers could have paid with cash or other means of payments).

All interested parties are invited to provide arguments in favour or against the liability of a Payment Service Provider towards the customers and/or the merchants in case of breakdown of a payment network, as well as any other suggestions in this area.