European Economic and Social Committee

ECO/172

Transfers of funds/
Information on the payer

Brussels, 21 April 2006

OPINION

of the

European Economic and Social Committee

on the

Proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds

COM(2005) 343 final - 2005/0138 (COD)

_____

99 rue Belliard - B-1040 Brussels - Tel. +32 (0)2 546 90 11 - Fax +32 (0)2 513 48 93 - Internet http://www.esc.eu.int

EN

On 26 September 2005 the Council decided to consult the European Economic and Social Committee, under Article 262 of the Treaty establishing the European Community, on the

> *Proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds*
> COM(2005) 343 final - 2005/0138 (COD).

The Section for Economic and Monetary Union and Economic and Social Cohesion, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 23 March 2006. The rapporteur was Mr Burani.

At its 426th plenary session, held on 20 and 21 April 2006 (meeting of 21 April), the European Economic and Social Committee adopted the following opinion by 85 votes to 15 with six abstentions.

*

* *

1. Introduction

1.1 The proposal aims to transpose Special Recommendation VII (SR VII) of the Financial Action Task Force (FATF) into Community legislation. This Recommendation was issued with the objective of "**preventing *terrorists and other criminals*** from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs"[1]. It is part of a series of laws and regulations seeking both to **freeze terrorists' assets**[2] and to **prevent laundering of the proceeds of *criminal activity***[3]**.**

1.2 Essentially, the measures proposed by the Commission are simple in form but substantial in content and in practical consequences. The proposal lays down **a requirement for payment service providers (PSPs)** – in practice the financial institutions which carry out transfers of funds – **to record information on the payer**: this information must **accompany the transfer of funds from the payer's PSP to the end recipient (payee)'s PSP**. The provision applies to **transfers of funds within the EU** and, with a number of exemptions and derogations, to transfers from and to third countries as well.

1.3 The EESC fully agrees that a regulation deriving its legitimacy from Article 95 of the Treaty is necessary; this solution has, moreover, received the preliminary agreement of the Member

1 FATF, "Revised Interpretative Note to Special Recommendation VII: Wire Transfer".

2 Council Regulations (EC) Nos 2580/2001 and 881/2002.

3 Directives 91/308/EEC, 2001/97/EC etc.

States and the PSP sector. There is general consensus that it would be appropriate to adopt a direct implementing instrument such as a regulation, rather than a directive, which would be likely to be implemented in different ways when transposed into national legislation. The measures provided for in the Commission document are, in general, appropriate and sensible, but the EESC **is concerned as to how effective they will be in practice**, at least in the short term.

1.4 Indeed, the EESC feels that the regulation has some weak points, both in that it provides for considerable individual assessment by PSPs and because it lays down technical procedures which are too open to evasion by criminals.

2. General points and comments

2.1 The fight against "*criminal activity*" (as organised crime is sometimes called in Community language, although it is high time that this euphemism were abandoned) was addressed systematically for the first time – at least in theory – by the 1996 Dublin Council, and an **Action plan** was adopted by the 1997 Amsterdam Council[4]. This comprised a series of 30 detailed, coordinated programmes which were to be completed by the end of 1998 at the latest; eight years on, the majority of them have yet to be implemented.

2.2 The concept of organised crime has evolved in successive stages. In 1998, OLAF[5] (then UCLAF) drew attention to the large-scale **tax evasion** affecting Community finances, **attributing it to organised crime**. The concept was expanded after the attacks on the Twin Towers and subsequent attacks, to focus particularly strongly on **terrorism**.

2.3 The same thought process and trend was followed concomitantly by the Financial Action Task Force (FATF) set up by the G8, which is still the most authoritative body uniting governments. Created to combat money laundering linked to organised crime, the FATF's **remit has now been extended to include *all* forms of terrorism-related financial activity**: its nine Special Recommendations (SR) are particularly important and the majority of them have been converted into Community provisions on money laundering and payment systems. The proposal in question implements SR VII on "wire transfers" carried out by terrorists "*and other criminals*".

2.4 Introducing the concept that criminal ***financial activities*** – whether related to terrorism or organised crime – are a **global phenomenon** and must be combated together would simplify the language used in the proposal; this is important not least for the purposes of combating the phenomenon *on the ground*. As things stand, at both Community and national levels, the focus is on either one or the other: the many initiatives adopted refer sometimes to "organised

4 Action plan to combat organised crime, OJ C 251 of 15.08.1997.

5 COM(1998) 276 final: Protection of the financial interests of the Communities - Fight against fraud - Annual report 1997.

crime, *including* terrorism" and sometimes to "terrorism *and other criminal activities*". It is not always easy – for the investigating authorities and still less so for PSPs – to classify illegal financial activities as belonging to a specific sector, particularly considering that **terrorism has forged close links with organised crime and vice versa** in a number of sectors: arms and drug trafficking, illegal immigration, counterfeiting of bank notes, document forgery and so forth.

2.5 When it comes to combating unlawful *financial activities*, therefore, organised crime and terrorism are **two sides of the same phenomenon**. The impression that this fact is not always acknowledged is given *not least* by the explanatory memorandum, which repeatedly mentions "**combating money laundering *and* terrorist financing**". Without as yet wishing to comment on the proposed measures, the EESC believes that this phrase is misleading. For reasons which will be better explained in the comments on the individual articles, it should be made clear that the text deals with organised crime and terrorism.

2.6 Furthermore, the FATF itself was originally behind the splitting of these two concepts: the title of the nine SRs referred to in point 2.3 is simply Terrorist financing; the title of the Interpretative Note to the SRs is Special recommendations on terrorist financing, but the text mentions "preventing terrorists *and other criminals* from having unfettered access …". The Commission has reproduced this distinction when transposing the FATF recommendation, and is including the regulation among the measures for **combating terrorism**. The EESC believes that the regulation should be seen as part of the series of more general measures to combat **money laundering and organised crime**. The distinction is not important from a legal point of view but it is important when it comes to practical implementation, as the following comments attempt to show.

3. Comments on the text of the proposal

3.1 **Article 2: Scope.** The regulation applies to transfers of funds to or from a PSP established in the Community and to payees or from payers established in the Community; it also applies (Article 7) to transfers from the Community to payees established outside the Community and to transfers to the Community from third countries (Article 8), with some adjustments.

3.1.1 The regulation does not apply to transfers of funds which flow from a ***commercial* transaction** carried out using a credit or debit card, provided that a **unique identifier**, allowing the transaction to be **traced back to the payer**, accompanies all transfers. *E*money (i.e. pre-paid card) transactions are neither explicitly excluded nor explicitly included. The PSPs will comment on the technical procedures; for its part, the EESC points out that the process for card transactions is the reverse of that for payment orders: the payer's PSP (which is sent a bank statement detailing the transactions made using the card) is not aware of the payee's activities or of the nature of the relationship between payer and payee. In the vast majority of cases, it will not only be **impossible to distinguish commercial transactions**

from non-commercial transactions, but also, often, technically impossible to identify the payer.

3.2 **Article 5: Information accompanying**[6] **transfers of funds.** PSPs have to include complete information on payers in payment orders, after ascertaining and **verifying that the information is complete and reliable**. However, for transfers of funds to payees outside the Community up to an amount of EUR 1 000, PSPs "may" determine the extent of such verification. While this flexibility is sensible and realistic, it also permits substantial financial outflows which **fall into the category of "immigrants' remittance"** but only appear to be going to the payer's family of origin. Moreover, the verification normally required for all other orders is problematic in the case of these kinds of transfers, which are often cash transfers and are carried out by a large number of private individuals through different PSPs, the identification of these individuals being of no particular consequence.

3.2.1 In any case, if orders of less than EUR 1 000 are to be exempt from monitoring, PSPs will have to put in place separate, costly, unnecessary procedures; it would be better for the text of the article to refer to the anti-money laundering provisions already in force as regards orders made by payers who are not current-account holders.

3.3 **Article 9: Transfers of funds lacking information on the payer.** Under Article 6, the PSP initiating the transfer has to provide the payee's PSP with information on the payer. Where this information is missing or incomplete, the payee's PSP has to request it from the payer's PSP: moreover, it can reject the payment, suspend it or perform the transfer under its own responsibility with due regard for anti-money laundering provisions. Should the occurrence be repeated, the payee's PSP has to **reject *all* orders from that PSP or terminate its business relations with it. The "authorities responsible for combating money laundering or terrorist financing" have to be informed** of the decision.

3.3.1 The requirement for one credit institution to suspend relations with another in the cases specified clearly raises the issue of *proportionality*: money transfers usually only account for a small part of relations between international credit institutions, which include credit lines, services, transactions in securities etc. for immeasurably higher sums than those involved in an unlawful – or supposedly unlawful – transfer of funds. *Immediate* suspension of relations, as proposed by the Commission, would cause huge, unjustifiable damage for both PSPs and their customers.

3.3.2 The use of the term "authorities responsible" raises the basic issue described in the introduction to this opinion. It should be borne in mind that the general anti-money laundering rules lay heavy responsibilities – including in terms of criminal liability – on PSPs and their

6 This footnote relates solely to the Italian text. Since the transfers in question are electronic, the author advocates using the word "inclusi" (literally "included") instead of the word "allegati" (literally "attached"). The footnote does not apply to the English version, which translates "allegati" as "accompanied".

staff. It is not always easy to tell, when a transaction is deemed to be "suspicious", whether it is attributable to "common" crime or terrorism. Each country has investigating and law enforcement authorities of various different kinds: criminal police (sometimes divided into two separate bodies), financial police, customs, secret services. Where no precise information is given, the PSP will have the task of identifying **the authority it should notify**. The regulation therefore requires PSPs to decide on issues which lie outside their sphere of professional competence.

3.3.3 A provision is therefore needed requiring Member States to **create a single contact point**, responsible for receiving reports and referring them to the competent investigating bodies[7]. Moreover, this measure was already envisaged in the Council's 1997 Action plan.

3.4 **Article 10: Risk-based assessment.** This article states that the payee's PSP is to consider incomplete information on the payer as cause for suspicion and to be reported to the responsible authorities. The provision gives the PSP the right to establish on a case by case basis whether it is a question of a mistake, an omission or a "genuinely" suspicious case: this may prove to be a hard task given that each PSP has to process a considerable quantity of transactions every day. Moreover, as regards reporting suspicious cases, the comments made in points 3.3.2 and 3.3.3 apply.

3.5 **Article 13: Technical limitations**. The provisions of this article relate to transfers from third countries: the payee's PSP has to keep the information on the payer for at least five years, irrespective of whether that information is complete or not. Where there is an intermediary PSP established in the Community, it is required to report the lack of complete information to the end PSP. Here the Committee would merely note that keeping information for such a long period of time could be a considerable burden and involve the accumulation of tonnes of information: this provision can only be justified if it is *genuinely* expected to be useful. It might be advisable to reflect on this point and only require information to be kept where sums exceed a specified amount.

3.6 **Article 14: Cooperation obligations.** PSPs are required to **cooperate** with the authorities responsible for combating money laundering or financial terrorism, **by supplying the data and information in their possession without delay**. Those authorities may use the information "*only* for the purposes of preventing, investigating, detecting or prosecuting money laundering or terrorist financing".

3.6.1 The EESC **fully endorses** these provisions. It has just one further comment to make in response to the demands from certain quarters which have **expressed reservations** regarding

7 The need for a single point of contact is not new – nor did the request originate with the EESC: it was already included in the Council's 1997 Action plan, referred to in point 2.1 above, under which each Member State was to create "*a single contact* point providing access to *all* the law enforcement agencies*"*. Many years later, this body still does not exist and cooperation between investigating and law enforcement bodies, at both national and Community levels, is still an issue which has yet to be fully resolved.

a potential dilution of the provisions protecting privacy. The greater interest of the community, which is engaged in combating an extremely serious threat to society, requires, in some cases, **departure from key principles** in order to ensure its protection. The obligation placed on authorities to use the information only for the specified purposes is in itself a safeguard against any abuse. It should also be borne in mind that people transferring funds to bodies pursuing "genuine" social or public-spirited ends have nothing to fear: this does not constitute tax evasion or breach of the law or a reprehensible action.

3.6.2 From another point of view, it should be asked how effective these measures are **in practical terms**. For PSPs, the general rule of "know your customer" should apply, exempting them from carrying out checks on and reporting customers whose trustworthiness is known and proven. However, although this rule is quite easy to apply where payees are concerned, it would be much more difficult and burdensome to check on payers, particularly where transfers are effected using the procedures laid down in point 3.1.1 above.

3.7 **Article 19: Transfers of funds to charitable organisations within a Member State. In derogation** from the provisions of Article 5, Member States may exempt PSPs from the requirement to comply with the provisions on supplying the payer's identification details where transfers are made to **organisations carrying out activities for charitable, religious, cultural, educational, social, fraternal or environmental purposes or promoting sustainable development**, provided that:

a) these organisations are subject to reporting to and supervision by a public authority or to external audit requirements;
b) transfers are limited to a maximum amount of EUR 150 per transfer;
c) transfers take place exclusively within the Member State.

3.7.1 The Member States which apply the planned exemption will certainly find it very challenging to keep a record of relevant organisations and monitor compliance with the rules. Furthermore, the PSP is supposed to verify, on a case by case basis, that the payer is included on a continually updated "whitelist": this is undoubtedly a burdensome requirement. However, the situation varies from country to country: in those countries where the regulations are inadequate, the condition referred to in point 3.7a) may prove difficult to respect.

3.7.2 The exemption granted by the proposal is based on the premise that the social objectives pursued by these organisations are in themselves a guarantee that the funds will not be misused. This is true of the majority of those organisations, of well-known organisations and of public disaster appeals, but it is also a fact that some of the smaller, less-well known bodies supposedly pursuing social or public-spirited ends are used by terrorists as a front. In relation to the activities referred to in the last part of point 3.7, the regulation cannot discriminate on the basis of religious faith; it is, however, a well-known fact that NPOs are sometimes an apparently harmless "front" for financing terrorism whose menacing nature only comes to

light subsequently. In short, alongside a majority of "transparent" NPOs, there are some others that need to be carefully monitored: the problem is how to pinpoint them.

3.7.3 The proposal also overlooks the possibility that NPOs might be a front for **criminal organisations** which are not necessarily terrorist organisations. The profits from small-scale drug-dealing, prostitution and racketeering can easily be passed off as donations to NPOs with appealing names whose representatives – at least as far as the PSP can tell – are completely above suspicion. In actual fact, indirect monitoring systems exist which can bring to light some suspicious cases: for example, frequent payments from the same individuals always made in cash are characteristic of these kinds of activities. These methods are well known to criminals, however, who take suitable precautions by breaking up payments, using a different PSP each time etc. Thus, frequent payments *always made by the same payers* could arouse the suspicion of a **payee's PSP**, in particular. However, with the current electronic storage systems this kind of monitoring could only be performed with *ad hoc*, customised programmes, and this is clearly difficult to implement.

3.7.4 The EESC therefore points out that **exemption** - which the regulation leaves PSPs to decide at their own initiative on the basis of the information in their possession regarding purpose, monitoring, trustworthiness of representatives etc. - is a **weak point in the system**. PSPs may be willing to cooperate but will never be able to do so sufficiently to curb money laundering and crime financing: first and foremost, the authorities themselves must play an active role and **report the names of suspects**. To this end, however, the idea of a central authority as discussed above must become reality.

3.7.5 The EESC has a further point to make to the relevant authorities. Except in the case of direct notification by PSPs, the information is kept for five years, in the main so that it can be referred to by authorities *to provide evidence for crimes which have already been committed*. It is therefore, for the most part, used *to provide evidence* and not for prevention or control measures. It is worth asking how, in practice, it will be possible to pick out individual cases from hundreds of millions of transactions which have been recorded over the years.

3.7.6 Lastly, it should be pointed out that the explanatory memorandum to the regulation does not make any attempt to set the **costs of the system** against the potential benefits. Not all PSPs have adequate facilities to comply with the provisions, and even those whose facilities are adequate will have additional burdens and organisational constraints to cope with. The cost of these will inevitably be passed on to all the users of the payment systems: this sacrifice is only acceptable if the new regulation can be shown to bring specific, tangible benefits.

Brussels, 21 April 2006

The President of the European Economic and Social Committee	The Secretary-General of the European Economic and Social Committee
Georgios Dassis	Patrick Venturini

*

* *

N.B.: Appendix overleaf.

APPENDIX
to the
Opinion of the European Economic and Social Committee

The following amendments, which received at least one quarter of the votes cast, were rejected during the plenary debate (Rule 54(3) of the RP):

Point 3.7.2

Amend as follows:

> *"3.7.2 The exemption granted by the proposal is based on the premise that the social objectives pursued by these organisations are in themselves a guarantee that the funds will not be misused. This is true of the majority of those organisations.~~, of well-known organisations and of public disaster appeals, b~~ But it is also a fact that some of them ~~smaller, less well-known bodies supposedly pursuing social or public-spirited ends~~ are used by terrorists as a front. ~~In relation to the activities referred to in the last part of point 3.7, the regulation cannot discriminate on the basis of religious faith; it is, however, a well-known fact that NPOs are sometimes an apparently harmless "front" for financing terrorism whose menacing nature only comes to light subsequently. In short, alongside a majority of "transparent" NPOs, there are some others that need to be carefully monitored: the problem is how to pinpoint them.~~"*

Reason

To be given orally.

Voting

For:	37
Against:	44
Abstentions:	8

Point 3.7.4

Amend as follows:

> *"3.7.4 ~~The EESC therefore points out that~~ Although the provisions relating to **exemption** – which the regulation leaves PSPs to decide at their own initiative on the basis of the information in their possession regarding purpose, monitoring, trustworthiness of representatives etc. – could be ~~is~~ a **weak point in the system**, they are warranted by the role NPOs play in a democratic society. PSPs may be willing to cooperate but will never be able*

to do so sufficiently to curb money laundering and crime financing: first and foremost, the authorities themselves must play an active role and ***report the names of suspects****. To this end, however, the idea of a central authority as discussed above must become reality."*

Reason

The additions provide sufficient explanation for the suggested deletions. There is strong opposition within NGOs to the rules proposed by the FATF. Furthermore, if the EESC were to express support for these rules it would create major problems for the Committee's relations with NGOs.

Voting

For:	43
Against:	52
Abstentions:	7