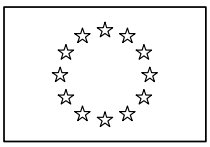

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 19.12.2006
SEC(2006) 1792

COMMISSION STAFF WORKING DOCUMENT

The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce

COMMISSION STAFF WORKING DOCUMENT

The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce

TABLE OF CONTENTS

1. INTRODUCTION

1. The confidence in and the stability of the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds. In the fight against this phenomenon, the European Community considered it appropriate to adopt, as a complement to the traditional criminal law approach, a preventive policy via the financial system. This preventive policy was initiated in 1991 with the adoption of Directive 91/308/EEC of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering[1]. The aim of the rules was to request the financial sector to identify their customers, to report suspicions of money laundering to the authorities and to establish appropriate internal procedures to guard against money laundering. This directive had, however, a limited scope of application in so far as it concentrated on the laundering of proceeds from certain criminal activity only (e.g. drugs trafficking).

2. In 2001 Directive 2001/97/EC[2] (hereinafter the "Second Directive") amended the preventive regime established by the 1991 directive by enhancing it. The goal was to adapt to the new money laundering methods and techniques that had appeared in the preceding years. Hereinafter, for the purposes of this document, all references to the "Directive" shall be understood to mean Directive 91/308/EEC as amended by Directive 2001/97/EC[3]. Although this Directive has been formally repealed by a new directive[4], this new Directive (so-called "Third Directive") builds on the previous one and does not substantially change the nature of the obligations of the legal profession in relation to the prevention of money laundering.

3. One of the most important underlying elements of the Directive is the requirement on the institutions and persons subject to the Directive (hereinafter "covered institutions and persons") to "know their customers". This is reflected, in particular (though not only), in the request to identify their customers (the so-called identification obligation). In this context, the Second Directive introduced some rules in relation to non-face to face situations. In the financial services sector, these are the situations where the customer is not physically present before the covered institutions and persons for identification purposes when entering into a business relation or performing a transaction. There are two main typologies:

   – (1) traditional non-face to face situation where the customer is simply absent at the moment of initiating a business relation;

---

1 OJ L 166, 28.6.1991, p.77.

2 Directive 2001/97/EC of 4 December 2001, amending the first anti-money laundering Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, OJ L 344/76 of 28.12.2001. Text available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32001L0097&model=guichett

3 For a consolidated version of the first directive (as amended by the second Directive), see: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/consleg/1991/L/01991L0308-20011228-en.pdf

4 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005.

– (2) the situation in which the customer is acting on behalf of a third party (either a natural or legal person[5]), the so-called economic beneficiary, who is not physically present. Two sub-situations are further distinguished: in the first case, the customer is physically present but not the economic beneficiary; in the second case, neither of the two is physically present.

In addition to these two main typologies, there is a sub-typology: the situation in which the customer has already been identified by the covered institution or person by virtue of a previous business relationship or transaction, but is not physically present for the purpose of carry out a particular transaction.

4. The examination. Article 2 of the Second Directive requires the Commission to carry out a particular examination of the aspects related to the identification of clients in non-face to face transactions and possible implications for electronic commerce. This document aims at replying to the call contained in the Second Directive, which the Commission committed to respect during the adoption of the Third Directive[6]. The Commission services carried out this examination in the autumn of 2005 by consulting stakeholders on this issue on the basis of standard questionnaires. Hence, the content of this document is based on the contributions prepared by a large number of Member States and several private entities from the financial sector in reply to those questionnaires. In addition, the Commission services used other available information in the preparation of this document.

5. This document presents the results of this examination regarding:

– (section 2) the transposition of the Directive at national level and the different approaches followed;

– (section 3) the most common specific measures adopted by the financial sector in order to cope with the risk in non-face to face transactions, as well as the most common problems in the application of those measures;

– (section 4) the impact of the measures adopted in terms of costs;

– (section 5) the effectiveness of the measures adopted with regard to the anti-money laundering defences and the financial system and the possible improvements in this regard.

Some conclusions will be provided in section 6. Finally, an appendix is added with perceived money laundering risks and countermeasures in electronic commerce.

---

5 When a person acts on behalf of a legal entity, the latter is not considered absent. Non face-to-face identification is needed in those cases only then when the authorised person is not present himself.

6 A parallel examination has been conducted in relation to the application of this Directive to the legal profession. The results of this other examination are presented in a different working document.

2. THE IMPLEMENTING LEGISLATION: NATIONAL TRANSPOSITION

2.1. The requirements of the Directive in relation to non-face to face situations

6. Article 3(11) of the Directive requires Member States to ensure that the covered institutions and persons take specific and adequate measures to compensate for the greater risk of money laundering which arises when establishing business relations or entering into a transaction with a customer who has not been physically present for identification purposes. In particular, non-face to face activities challenge the capacity of the existing measures to ensure appropriate identification of the customer (and of the third parties on whose behalf the customer may be acting), thereby bearing a risk of anonymity or false identity. Indeed identity theft in the financial sector is a growing concern in Europe[7].

   This greater risk of course would undermine the appropriate application of the other anti–money laundering measures based on customers' knowledge. Moreover, it is noted that when non-face to face activities are carried out in electronic commerce operations, risks increase (e.g. due to ease of access and speed) [8]. Specific risks in relation to electronic commerce are dealt with in the Appendix.

7. While the Directive requires that the measures to be adopted ensure that the customer's identity is established, it does not indicate mandatory measures to be applied. Some examples are nevertheless provided in the Directive: requiring additional documentary evidence; supplementary measures to verify or certify the documents supplied; confirmatory certification by an institution subject to the Directive; or requiring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution subject to the Directive.

8. No distinction is made among the different situations where the customer may be operating on a non-face to face basis. In particular, adequate identification measures must be applied regardless of whether the absent customer is entering a business relationship or is carrying out a relevant transaction. It is up to Member States to devise appropriate measures for each case, provided that those measures are adequate to compensate for the greater risk of money laundering deriving from non-face to face activities. It should be equally underlined that the covered institutions and persons should take specific account of these measures in their internal control procedures laid down in accordance with Article 11(1) of the Directive.

---

7 Identity theft is generally defined as the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name. Identity fraud is sometimes used as a synonym, although the concept of identity fraud also encompasses the use of a false, not necessarily real, identity.

8 The Directive is assuming that there are some risks which belong to the very nature of the non face-to-face situations. Some respondents have questioned the assumption that non face to face activities are to be considered *per se* risky. They observe that in several instances (such as transactions related to electronic commerce) checks and balances are in place which can reduce drastically the exposure to misuse (as regards e.g. limitations to the amount involved, the need to channel transactions through institutions covered by the anti – money laundering legislation). In this context, the level of risks should be assessed taking account of further circumstances (the pattern of the transactions executed is often mentioned).

2.2. Transposition in the Member States: the different approaches

9. The responses received show that the majority of Member States have enacted provisions specifically dealing with non-face to face identification[9]. Specific measures for non-face to face identification may be established in the law, in bylaws, or through a mix of instruments. In this latter case, the law identifies general safeguards, whereby secondary legislation or guidelines provide for more detailed or additional measures.

In those countries where specific provisions have not been adopted, this normally means that either this kind of identification is not permitted (the customer has always to be identified personally) or non-face to face activity triggers the same identification procedure as the one applicable for ordinary activity.

10. There are three main approaches in the way Member States have implemented the Directive obligations:

- (1) Non-face to face identification is not permitted;
- (2) Non-face to face identification is permitted and specific applicable measures are indicated in the legislation, including exceptions and derogations for situations where risks are considered to be too high and personal identification is required;
- (3) A risk-based approach is adopted, whereby specific measures are not mandated and non-face to face identification has to be carried out by the covered entity having regard to the actual risk.

11. Approach 1: Non-face to face identification is not permitted. Some countries (notably the Czech Republic, Germany, Hungary and the Slovak Republic) do not allow for non-face to face identification (this situation may also be the result of national legislation not containing specific measures in relation to activities performed by customers *in absentia)*. In these countries, however, a reliable third party is sometimes allowed to personally identify the customer on behalf of the covered institution or person. This third party may be, for instance, a financial institution, a notary, a diplomatic authority or other sufficiently reliable persons under a contractual relationship. This case is not a genuine non-face to face identification, since the customer is physically present *vis-à-vis* the third party.

Box 1 – Identification by qualified third parties: Germany

In Germany, a non-face to face business relationship may be established by engaging "reliable third parties". Third parties may be credit institutions, insurance companies offering life insurances or accident insurances with premium refund, notaries, embassies and consulates of EU member states, or Deutsche Post AG executing the standardized PostIdent Service. Additionally, third parties may also be other persons who are engaged on a contractual basis and sufficiently reliable. In particular, the third party has to ensure that its staff is adequately reliable, informed and trained in anti-money laundering issues. These requirements are subject to internal and external auditing. The ultimate responsibility for a correct identification and verification always remains with the original institution or company and cannot be shifted to the third party.

[9] At the time of the consultation specific legislation were pending before the competent bodies and were expected to be enacted early in 2006 (France, Denmark).

12. Approach 2: Non-face to face identification is allowed with exceptions or derogations. Several Member States provide for the possibility to identify the customers on a non-face to face basis, normally as an exception to the general rule of personal identification and provided in some cases that certain safeguards are applied: e.g. an obligation to physically identify the customers who have entered a business relationship at the first subsequent transaction is imposed in Latvia or an obligation to acquire, within a certain period of time, a copy of the customer's identity document is imposed in Spain.

13. However, non-face to face identification may be prohibited in circumstances regarded as particularly risky. These specific prohibitions are:

- Third parties business introducers. In some countries it is not possible to operate on behalf of third parties on a non-face to face basis, at least with regard to some kinds of transactions.

- Opening of a first business relationship. In some countries, only non-face to face transactions with an already identified customer within a business relation would be allowed. In this case, identification and verification procedures aim at ensuring that identity data acquired subsequently match with those collected before. However, the initial identification (e.g. the opening of the business relation), would require that the customer is physically present.

- Customers not eligible. Some countries put limitations or ask for additional safeguards in relation to the customers who can avail themselves of the non-face to face identification procedures. For example, customers having the head office or residence in a non–cooperative country (unless some specific safeguards are fulfilled, like a written confirmation of another credit institution with which the customer has established a permanent business relationship); or non-public or non-regulated organisations.

- Other cases where non-face to face identification is prohibited and personal identification is required include the use of cash, transactions in bearer securities, foreign legal persons that do not or must not perform commercial or manufacturing activities in the country where it is registered.

Box 2 – Exceptions or derogations to non-face to face identification.

In Belgium, identification by a third party business introducer has to be done on a face to face basis (prohibition of non-face to face identification), and final responsibility lies with the entity using the third party business introducer.

In The Netherlands, institutions are allowed to establish the identity of a client who does not appear in person if no cash is involved in the transaction. The first payment with respect to the service is made through an account which the client holds with a credit institution which has its registered office in one of the Member States and possesses a permit from the competent authorities of that Member State to carry out its undertaking, or in a state designated by the competent Minister.

In Slovenia, as far as non resident clients are concerned, non-face to face identification only applies to (non resident) Slovenian citizens and to (non resident) citizens of other countries, provided that those countries pay regard to standards in the area of prevention and detection of money laundering. The Minister of Finance is authorised by the law to draft a list of relevant countries.

14. Even in situations where non-face to face identification is normally permissible, personal identification may nonetheless be required (including by renewing the procedure) to complement the outcome of the non-face to face procedure when specific risks arise in concrete cases: for instance discrepancies in the information collected or available, risks higher than average, or attempts to avoid direct identification or suspicions.

15. Approach 3: Risk-based approach to non-face to face identification. In a few countries (such as the United Kingdom) national legislation does not provide for an explicit list of cases eligible for non-face to face identification (at the same time establishing exceptions or derogations), nor does it set out specific prescriptive measures in relation to customers operating on a non-face to face basis; rather, covered institutions and persons are required to identify themselves the appropriate measures in view of the existing risk. It is observed that this risk-based approach to identity checks is very much in line with the need for businesses to develop their methods of working, at the same time allowing for not too onerous procedures.

Box 3 – Risk-based approach to non-face to face identification: the United Kingdom.

An overall risk-based approach is in place in the United Kingdom, where further identification is required for non-face to face transactions and some acceptable standards are set out at the guidance level (e.g., voter's roll, credit bureau checks, copies of utility bills, bank statements indicating a home address). In particular, firms consider the overall risk posed by the customer, including location, customer behaviour, how the customer comes to the firm, and the products/services that the customer is using. In this framework, firms take into account the greater potential for money laundering which arises when a person is not physically present for identification purposes.

16. In other countries there is a sort of "mixed" approach where typical measures are identified in the legislation, but at the same time covered entities are required to apply them under a risk-based approach (as to the appropriate combination of tools and measures)[10]: for instance, the Belgian legislation requires the adoption of customer acceptance policies where the consideration of the risks plays a major role; while the Spanish legislation requires an assessment of the customers' risk to be carried out and, if that is higher-than-average, to apply appropriate measures. These obligations include, but are not limited to, non-face to face activities.

3. THE MOST COMMON MEASURES FOR NON-FACE TO FACE IDENTIFICATION AND THEIR PROBLEMS

3.1. The most common measures applied by the financial sector for non-face to face identification

17. Concerning the most common measures and procedures used in the Member States for non-face to face identification, it appears that they are very much in line with those indicated in the Directive as examples, although concrete modalities can vary

[10] In France there is a reference to the need to take account of the higher risk inherent in non-face to face identification, while the forthcoming decree will set out a number of typical measures, along the lines of those indicated in the second Directive (most common measures currently applied by credit and financial institutions include the acquisition of a copy of an official identity document or an official certificate of incorporation and a certificate of domicile).

from country to country. In this respect, three main categories of measures can be easily identified in national regimes.

– a) Identification through additional documentary evidence or supplementary measures to verify or certify the documents supplied. This generally implies that the customer, after having provided his identity data and the relevant documents on a non-face to face basis, is required to produce additional or supplementary documents to validate his own identification: for instance, the Spanish legislation requires covered institutions and persons to obtain from the customer, within a specified period of time, copies of relevant identity documents; while the Cypriot legislation requires that the customer supplies the financial institution with original documentary evidence (e.g. passport, national identity card), which is subsequently returned by registered and secured mail and also requires the financial institution to ensure telephone contact with the customer before opening the account on an independently verified home or business number. In other cases, the obligation to obtain additional or confirmatory evidence can be fulfilled by the covered institution or person through a variety of possible sources, such as access to relevant registers.

  The domestic legislation can indicate specifically which documents can be used to verify the identity of a remotely identified customer (e.g., electronic identity card, a qualified certificate within the meaning of the legislation on electronic signatures, a copy of another probative document). On the assumption that different types of documents do not present the same degree of reliability, instructions are also given in some countries (for instance Belgium) as to the supporting measures which can be taken to properly verify the identity and to further source where to get the information which are not included in the documents (e.g. the address).

– b) Identification through confirmatory certification by an institution subject to the Directive. This procedure is particularly common. In some cases, the institutions which can issue the confirmation also include entities which, although not subject to the Directive, are situated in third countries which impose equivalent requirements or which are designated by national competent authorities. Modalities of documental confirmation can differ from country to country. Direct confirmation of the prospective customer's true name, address and signature from a bank operating in his/her country of residence and an introduction letter from a professional intermediary (lawyer or accountant or other) are two examples. There are cases (for instance in Italy) where the customer can be introduced, for identification purposes, by another institution through a form indicating relevant information. It is also frequent that diplomatic or consular authorities can identify and certify customers' identity vis-à-vis covered institutions or persons.

– c) Identification by requiring that the first payment is carried out through an account opened in the customer's name with a credit institution subject to the Directive. This is also a quite common measure. It can be applied as a stand alone tool or in conjunction with other measures. There are examples where the use of a bank account to execute payments allows for an alleviation of other measures (for instance, in Luxembourg, a simple copy of identification documents instead of certified copy would be acceptable in this situation). In Italy, the law provides for a "suitable declaration" released to the covered entity by another financial

institution which, in turn, has identified the same customer, provided that the same customer has been identified on a face to face basis and the business relationship is existent when the payment is executed or the certification is issued.

18. In most cases, the measures identified by the national legislation for non-face to face identification are often considered to be equally reliable and, therefore, they can be applied alternatively. Nevertheless, caveats are also expressed to ensure that more than one measure is applied when that is appropriate to tackle specific risks. It may happen that some measures are intended to be applied in a cumulative way: e.g. the use of an existing account in the customer's name with a credit institution subject to Financial Action Task Force or equivalent identification requirements. There are also countries where different measures apply to different categories of eligible customers.

19. Some countries provide for additional (and less common) measures to ensure appropriate non-face to face identification in relation to specific risks. In this respect, electronic signatures appear to be increasingly used in several countries as an alternative to the acquisition of the identity data through traditional documents, also in certified form (for example in Belgium, Spain or Austria). Electronic signatures are also used in the United Kingdom in the framework of the risk-based approach to non-face to face identification. A proposal for internet-based "Know-Your-Customer" procedures relying on digital signatures is currently under discussion in Germany. Discussions on the suitability of electronic signatures for anti–money laundering purposes, in relation to identification in non-face to face activities, are also held in France.

It should be noted in this context that the electronic signature[11] has been developed as an instrument to facilitate electronic commerce and distant communications, with a view to ensuring that the transactions performed are secure and can have legal force. It has not been introduced specifically as a means to prevent money laundering in non-face to face activities by ensuring that the customer using it is actually properly identified. Therefore, the use of the electronic signature for identification purposes should be carefully considered in this framework.

Box 4 – Use of electronic signature: Belgium.

The Belgian legislation has introduced a rather detailed regime. Non-face to face identification through electronic signature can be conducted on the basis of "a qualified certificate", in the sense of the relevant national law and EU provisions. Moreover, this qualified certificate must be issued by a certification service established in a Member State of the EEA and accredited for the purpose in accordance with the provisions of the European Directive on electronic signatures, or other certification services with equivalent qualifications.

As to the procedure for issuing the qualified certificate of identity, it has to entail face to face identification of the customer by the certification service itself or, in accordance with its procedures, a

[11] Electronic signature, according to the EU legislation and the domestic implementing provisions, implies that the identity of the entitled person is verified and certified previously, by qualified and reliable parties, and that the signature itself is accompanied by secure information technology devices in order to ensure that it cannot be used by unauthorised persons. Particular attention is paid to the entities which can issue the certification on the identity prior to the attribution of the electronic signature (those entities should be qualified in anti–money laundering terms) and to the modalities with which that certification is performed (it should be done on a face to face basis).

person it empowers for that purpose. The qualified certificate must not be issued under a pseudonym; the institution obliged to identify the customer has a duty to verify, systematically and automatically, whether the certificate presented has not lapsed or been revoked by the certification service that issued it.

In the same perspective, the institution is required, on the basis of an update of the information it retains, to periodically review its decisions to admit certificates issued by the certification services which are not established in a Member State of the EEA.

3.2. The most common problems linked to the application of the measures.

20. The application of the measures for non-face to face identification generally gives rise to three main types of problems in relation to: (a) data protection legislation; (b) reliance on third parties; and (c) difficulties in obtaining information.

21. a) Data protection legislation. Non-face to face identification measures are very much based on the acquisition and management of identity information in different stages of the process (identification, verification) and from different sources (the customer himself/herself, external databases, other institutions or persons). The need to comply with data protection requirements is frequently mentioned by stakeholders as putting obstacles in the path of the collection and processing of information on customers' identity. In some cases, conflicts might even arise between data protection restrictions and identification measures related to the collection and management of information on customers. This is particularly true when identity data obtained from relevant documents on a non-face to face basis must be completed through the acquisition of further personal information from other relevant sources (e.g. population registers) or when additional documentary evidence must be collected or supplementary measures to verify or certify the documents supplied must be applied. As a result the procedure is more complex and burdensome.

22. b) Reliance on third parties. Mechanisms based on reliance on third parties, upon which rest many of the measures devised in national systems to tackle the enhanced risks in non-face to face activities, are particularly affected. Flows of information between different qualified institutions are essential in order to ensure the exchange of sensitive and appropriate information on customers' identity and profile. However, there are two major obstacles in relation to data protection restrictions, which impede the effective functioning of the mechanism:

- 1) Normally, banks are not compelled to provide other covered entities with information on the accounts opened by their customers. Furthermore, banks, even when allowed to do so, are very often reluctant for obvious commercial reasons (i.e. they are possibly favouring a competitor in getting a customer);

- 2) Should banks be permitted and willing to provide identity information on their customers to other covered institutions, data protection limitations may apply. This is the case either when the third party is asked to transmit information to the covered institution on customers' identity or when that information is embodied in the payment executed through an account open by the same customer within the bank.

23. c) Difficulties in obtaining information. Specific situations are mentioned by stakeholders where difficulties exist in relation to the acquisition of information

needed to carry out or complete (possibly, in the verification stage) the identification process. Indeed, some documents are difficult to obtain (though this also applies to normal face to face identifications): for instance, there are practical difficulties in obtaining information on the identity and the power of attorney of persons operating on behalf of legal persons, especially in relation to large companies which empower several persons to act on their behalf through bank accounts and, more generally, in the financial markets.

4. COST OF NON-FACE TO FACE IDENTIFICATION

24. Non-face to face identification normally implies additional costs for customers, covered institutions and persons, and for the system, in particular deriving from the steps taken at the initial moment of entering into a business relation. Indeed, depending on the types of transactions carried out, distance operated transactions may provide substantial savings to the financial institutions later on.

– The additional cost for the customer may relate in particular to measures requiring additional expenditure on documentary evidence, such as authentication of documents by notaries, etc.

– In the case of individual institutions and persons, respondents observe that national provisions on identification measures are often quite detailed and prescriptive, leaving little room for the flexibility needed to take account of different circumstances and to keep costs as limited as possible. As a result, non-face to face procedures may be slow and costly. In some instances they have felt it necessary to purchase expensive software systems to assist with checking and this has significantly increased the overall costs of compliance.

Box 5 – Examples of costly identification measures

Stakeholders note that the implementation of identification measures requires procedures, training, systematic controls by service offices, tools of detection (implementation time and costs, project management), a specific compliance committee for the examination of large risks, regular communication concerning the required authorization process involving high management.

– The cost for the system relates in particular to the duplication problem. Since similar identity checks are mandatory for each of the financial institutions intervening in the chain of financial services provision, duplication of interventions are very likely to occur in the application of identification measures with respect to the same customers. As a consequence of these duplications, as well as of other factors which increase the difficulties in acquiring relevant and complete information on customers (especially those operating in a corporate form or under other legal arrangements), costs and organisational burdens are often perceived by stakeholders as too high, for little discernable benefit. This has a further impact on the effectiveness of the system (see below).

Box 6 – Situations of duplication procedures: the card issuer example

The subsequent intervention of different covered institutions or persons for the identification (and overall "Know Your Customer" or "Customer Due Diligence" screening) of the same customer is a common situation in activities related to the issuance and use of means of payment, electronic money

and other means of payment suitable for electronic commerce and other transactions typically executed on a non-face to face basis. This is particularly the case of financial institutions (as opposed to banks) issuing credit or charge cards, which normally operate on a non-face to face basis, certainly in relation to the transactions performed by the customers. In this context, the card issuer is required by legislation to obtain and keep copies of identity documents from the customer, which results in delays and additional steps in the process of issuing cards. However, normally the card holder has already acquired a bank account, used by the card issuer to regulate the expenses; the bank has therefore already identified that customer and carried out the appropriate screening procedures.

Stakeholders note that banks are in a better position to acquire and keep all customers' information, given also the branch network and the personnel specifically devoted to following the customers' activities. Furthermore, as deposit taking institutions, banks can monitor customers' activity. Stakeholders believe that the real contribution cards issuers may give to money laundering prevention and detection is not by monitoring a business relationship (as banks can do) but rather by analysing the transaction pattern or payment behaviour of the credit/charge account.

5. EFFECTIVENESS: THE NEW CHALLENGES

5.1. General perception

25. On the one hand, additional measures applicable for non-face to face activities, given the increased burden they pose, can entail a deterrent effect on covered institutions: in marginal cases, non-face to face procedures can also have a dissuasive impact on decisions concerning the marketing of specific products or even the acceptance of particular customers. These effects are obviously difficult to measure.

26. On the other hand, one should not lose sight of the ultimate goal of the anti-money laundering rules in this regard which is to "Know Your Customer" and to act in accordance with this knowledge. From this perspective, it would make sense to question whether the measures on identity checks which are currently applied across the board could be improved. In this context, the effectiveness of the system is also linked to the cost considerations (above), certainly from the perspective of the financial sector. The general perception from stakeholders is that current non-face to face identification measures are not cost effective.

Two main solutions are identified by stakeholders as possible tools to explore in order to alleviate costs and burdens for covered institutions and at the same time increase their efficiency; while ultimately enhancing the effectiveness of the system:

– (1) instead of a "one size fits all" approach as regards identification measures referring to all covered entities, different institutions could be given different roles, depending on the activities they carry out;

– (2) implementing a meaningful risk-based approach would grant a higher degree of flexibility, whereby resources could be concentrated on the situations which require enhanced attention or scrutiny.

Not surprisingly, this assessment is also found in the roots of the recently adopted Third Directive[12] in the field of anti-money laundering. There are, therefore, two main challenges for the future years: reliance on third parties and the risk-based approach.

5.2. Different roles for the institutions: exhausting the possibilities to rely on other financial institutions. Knowing your customer, from identity checks to monitoring of transactions

27. Stakeholders are of the view that different financial institutions should be given different roles, depending on their position in the chain. This approach generally implies a strong role for banks in relation to the customer identification procedures and a reliance mechanism. For example, a complete identification would take place when opening a bank account, whereby the subsequent issuance of a credit card by a different financial institution to the same customer (to be used through that account) should induce a reliance mechanism on the identity information already collected by the bank.

28. The different roles played by the financial institutions are indirectly recognised by the Third Directive when it allows Member States to permit the establishment of reliance mechanisms of this kind. However, the Third Directive does not contain an obligation for Member States to apply the reliance provisions (so-called performance by third parties). Therefore, it is yet to be seen what the concrete impact of the new measures will be.

29. Stakeholders anticipate that the challenge will be to exploit the possibilities of the reliance mechanisms so as to allow for moving from the "identity checks" scenario to the "monitoring of customer's transactions and profile" scenario for the purposes of knowing the customer. They claim in this context that existing duplications prevent some institutions from effectively focusing further on mechanisms and processes to know the customer and to prevent money laundering, such as accounts' pattern analysis and transaction monitoring. For instance, stakeholders consider that screening processes and systems to monitor fraud operated by card issuers provide useful tools for appropriate customer due diligence procedures and high quality safeguards against money laundering. Similar considerations apply to electronic money issuers. They occupy the position of intermediary in the payment process and are often able to provide additional transaction information to law enforcement investigations that complements verification of identity data provided by the underlying financial institutions. This transaction information may be more valuable in managing the risk of money laundering than, or equally valuable to, a repetition of verification of identity as it can yield valuable information to assist law enforcement in the event of investigation.

5.3. Enhancing flexibility: the risk-based approach

30. The Second Directive did not, as such, establish a requirement on covered institutions and persons to adopt a risk-based approach in relation to the

---

[12] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L309, 25.11.2005, p. 15.

identification of their customers. However, it provided for a limited risk assessment to be made by Member States, which were required to take "specific and adequate measures" in order to compensate for the "greater risk" of money laundering entailed by non-face to face situations. In practice, a number of respondents to the consultation showed that a risk-based approach to non-face to face identification has, to some extent, been applied in the implementation of the Second Directive to date.

31. In this respect, it is noted that a fully–fledged risk-based system would mitigate the rigidities described in the precedent sections and would allow the measures and procedures to be tailored in a more appropriate way. This would favour a more cost-effective system of non-face to face identification, where different situations and roles played by the institutions and persons involved would be adequately taken into account.

The possibility of applying particular diligence in cases of higher risk would also allow, in particular, the financial institutions (as well as their supervisors) a flexible response to new situations, while taking into account different vulnerabilities.

32. The advantages of applying a comprehensive risk-based approach are recognised in the Third Directive, which allows the covered institutions and persons to determine the extent of the measures related to customer due diligence procedures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction (Article 8(2). It must be noted in this context as well that the Third Directive has not changed the assumption that non-face to face situations would entail a higher risk (Article 13(2)).

33. Therefore, the challenge will rest with the practical implementation of the risk-based approach. For stakeholders, it is not the fact that transactions are conducted without personal contact between a financial institution and its customer which increases risk of money laundering (that would be too formalistic an approach). Rather, this risk increases where the knowledge on the customers' background and profile is poor. This problem can be and is addressed by monitoring systems which are aimed at detecting patterns of unusual financial behaviour which, on the basis of experience and available information, are likely to be connected to money laundering activities. The quality of the indicators for such unusual behaviour is critical. In this regard, stakeholders consider that input from law enforcement authorities is indispensable.

It is observed in this context that a risk-based approach also implies obligations for the parties involved. It also puts a premium on ensuring that there is broad equivalence of implementation of risk-based policies in similar situations. For this, it is not just rules that will be needed, but also sound coordination on the assessments of the risks involved among the financial service sector(s) concerned, between the firms and their supervisors, as well as among supervisors at international level.

6. CONCLUSION

34. The issue of non-face to face identification is a multi-faceted one. There is a number of circumstances where customers may be operating without being physically present vis-à-vis the covered institution or person. Relevant situations range from clients asking to open an account using distant banking facilities, to beneficial owners being

represented by a third party, to already identified customers executing a transaction remotely.

In general, non-face to face situations entail a greater risk of anonymity, whereby the Anti-Money Laundering system rests upon sound "Know Your Customer" policies, based in the first place on appropriate client's identification and on the capacity to follow the paper trail. However, different non-face to face activities bring about diversified risks, as far as intensity and nature are concerned. For these reasons, the second Directive adopted a flexible approach: without providing for specific (and, thus, rigid) provisions Article 3(3) mandates Member States to adopt "specific and adequate measures necessary to compensate for the greater risk of money laundering which arises" in such cases.

35. In such an open and flexible framework, appropriate implementation requires an effort from Member States in identifying relevant situations, assessing the risks and devising the most appropriate measures to tackle them. Member States' responses have indeed been diversified. Different approaches have been taken at national level in regulating identification in non-face to face situations. These approaches range from the prohibition of non-face to face identification, to the provision of specific measures and procedures to address this kind of identification, in some cases within an overall risk-based system.

Although compliance is difficult to assess, precisely because of the flexible nature of the obligation at stake and of the variety of solutions adopted by Member States, the level of implementation can be judged as adequate. No major loopholes appear from the overview conducted; the risk of anonymity seems to be in general appropriately managed and adequately mitigated.

36. In this context, according to responses received from the private sector, the measures applicable to non-face to face identification are sometimes affected by a certain degree of rigidity. This is perceived as a complicating factor by institutions providing their services on a non-face to face basis; procedures in place have to take account of the need to obtain additional evidence, thus increasing costs and operational burdens for compliance.

It is observed, in this perspective, that a significant simplification would be easy to achieve, at the same time maintaining the capacity of managing risks and valuing different roles played by different institutions. In particular, where more institutions intervene in the provision of services to the same customers, reliance could be made to the identification carried out by the first in the chain: this would avoid duplications and focus resources for anti-money laundering where they would be most useful.

On the other hand, it is observed that many procedural complications derive, in non-face to face identification, from the need to acquire information from identity documents or other sources of identity information. In this respect, electronic signatures, if appropriately implemented and taking into account anti-money laundering needs (e.g.: the issuer of the certificate has to identify the customer on a face to face basis), would be particularly helpful in speeding up the process and, at the same time, ensuring the same (if not higher) level of reliability.

37. The Third Directive fits into the existing scenario on non-face to face identification. While an overall risk-based approach is introduced, non-face to face activities, as intrinsically risky, trigger the application of enhanced customer due diligence measures. These measures are, in many cases, consistent with those introduced by Member States in the implementation of the second Directive. Nonetheless, the new regulatory framework will have a significant impact both on Member States and on covered institutions.

38. Countries will have to complete the regulation applicable to non-face to face identification aligning the measures in place to the new provisions. In particular, attention will have to be paid, on the one hand, to the implementation of an overall risk-based approach and, on the other hand, to the transposition of the concrete measures indicated in Article 13(2) of the Third Directive for non-face to face situations.

The implementation of the Third Directive in this respect will not impose a change over to a completely new system: not only was the consideration of the "greater risk" built into the second Directive, but also many of the measures in place fit well into the new scenario. Indeed, the replies received and the overview carried out in the previous paragraphs show that there are measures already in place in some cases such as: the acquisition of additional documents or information to establish customers' identity; supplementary measures to verify or certify the documents supplied (including through confirmations issued by credit or financial institutions) or payments received through an existing account of the same customer.

39. Also in this respect, the implementation of the Third Directive will provide opportunities to increase the efficiency and the effectiveness of the system. In particular, it is worth underlining that customer due diligence procedures based on third parties acting as introducers and on the possible reliance on the identification performed by them offers an opportunity to take account of different roles played by credit and financial institutions in the distribution of financial products.

APPENDIX - PERCEIVED MONEY LAUNDERING RISKS AND COUNTERMEASURES IN ELECTRONIC COMMERCE

1. In most cases, national legislation does not contain anti-money laundering measures specifically dealing with electronic commerce. Many respondents note that electronic commerce transactions are not risky *per se* and that institutions issuing e-money or other means of payment used for electronic commerce are subject to the anti-money laundering measures. For instance, issuers of electronic money typically occupy the position of intermediary in the payment process, sitting between two existing financial or credit institutions. Their infrastructure is built onto the existing credit card and bank account systems. This adds greatly to its security and acts as a significant mitigant to non-face to face concerns.

2. The main risk factor is in the identification stage, since electronic transactions are mostly conducted on a non-face to face basis. Therefore, the measures taken to appropriately identify the customers are also relevant to tackle the issue of electronic commerce. In this context, the measures on non-face to face identification described in this report are fully relevant.

3. However, it is also observed that, although applications and transactions undertaken across the Internet may in themselves not pose any greater risk than other non-face to face business, some factors may aggravate the typical risks. Those factors include ease of access to the facility, regardless of time and location; the ease of making multiple fictitious applications; the absence of physical documents and the speed of electronic transactions. Moreover, electronic commerce transactions pose increased difficulties in understanding the nature and purposes of the transactions as well as in making sure that the person who operates is actually the identified customer. This is also linked to the problem of identity theft.

4. Recognising these difficulties, the Commission has recently launched a call for tenders (MARKT/2006/08/F) for a study on user identification methods in card payments, mobile payments and e-payments, which are the most widely used methods for electronic commerce. The results of the study will be known in 2007.

5. It is also noted that measures aimed at identifying the parties involved in wire transfers are also particularly relevant in providing anti-money laundering safeguards in electronic commerce operations, in relation to the payment phase. This issue is now tackled in a Regulation adopted on 15 November 2006[13].

[13] See Regulation (EC) No1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L345/1, 8.12.2006.

Box 7 – Measures in relation to electronic commerce

In some countries, measures are in place to specifically address the activity of e-money institutions or which have a direct relevance for the use of electronic commerce instruments.

In Belgium, customers entering business relationships with the sole purpose of issuing and using electronic money do not have to be identified if the capacity of the electronic carrier is limited to a maximum of 150 euros. If the customer subsequently requests reimbursement of more than 10 euros, identification is needed.

In Spain, the movement of any material support, including electronic support designed for use as a means of payment in an amount greater than 6.000 euros (for foreign transportation) or 80.500 euros (for domestic transportation) triggers the obligation to declare the origin, destination and current possession of the funds (registered credit or debit cards are not included).

In France, specific obligations are imposed on e-money institutions: internal controls must include identification procedures; automatic systems must be in place to detect anomalous use of e-money; internal rules must specify the measures applicable in relation to anomalies of interest for money laundering prevention; e-money instruments which do not allow the identification of the user cannot exceed 150 euros and 30 euros is the maximum amount for each transaction; e-money issuers must ensure traceability of transactions for two years.

A secure electronic signature is also seen as a valuable tool to ensure adequate anti-money laundering safeguards in electronic commerce transactions. However, it is noted by a firm operating as a credit card issuer, that the only country where a real electronic signature process can be used is the United Kingdom (as a consequence of the relevant regulations issued with the new Consumer Credit Contract Regulations in 2004), while in other Member states the electronic signature process is still complex and cumbersome.