Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

Review of the FATF Forty Recommendations

Consultation Paper

30 May 2002

The FATF invites comments on this Consultation Paper.
Comments should reach us by **31 August 2002**.

You can send your response by e-mail
or in writing to the following address:

FATF Secretariat
2, rue André Pascal
75775 Paris Cedex 16
FRANCE
Telephone: 33 1 45 24 89 67
Fax: 33 1 45 24 17 60
E-mail: Contact@fatf-gafi.org

If you have specific questions concerning the issued raised in the Consultation Paper or the review process please contact the FATF Secretariat

The Review of the FATF Forty Recommendations

Consultation Paper

Paris
30 May 2002

FATF Secretariat
2, rue André-Pascal
75775 Paris Cedex 16
France

TABLE OF CONTENTS

Annexes

1. EXECUTIVE SUMMARY

1. The FATF Forty Recommendations have been endorsed by more than 130 countries, are widely accepted as the leading international anti-money laundering standard, and have been, or are being, successfully implemented. However, money laundering methods and techniques change as new measures to combat money laundering are implemented and new technologies are developed. In addition there have been several developments at an international level, such as the U.N Convention on Transnational Organized Crime, the amendments in Directive 2001/97/EC of the European Parliament and of the Council, amending Council Directive 91/308/EEC dealing with money laundering, and the creation of the FATF Special Recommendations on Terrorist Financing. All these factors have made a review of the Recommendations desirable.

2. The FATF has identified a number of areas where possible changes could be made to the FATF framework, and these are set out in detail in Sections 3-5 below. The broad topics covered concern customer due diligence and suspicious transaction reporting, beneficial ownership and control of corporate vehicles, and the application of anti-money laundering obligations to non-financial businesses and professions. Each topic sets out the nature of the problem or issue, identifies the risks, outlines the current position, and provides one or more options or alternatives for dealing with the issue or risks.

Section 3

3. Section 3.1. of the paper commences by clarifying the meaning of "financial institution", as used in the FATF framework, by reference to a range of financial activities. This is important as the Recommendations currently contain a range of obligations that apply to financial institutions, such as customer identification, record keeping, reporting of suspicious transactions and internal controls.

4. Section 3.2. recognises that customer due diligence is an important component of any financial institution's anti-money laundering (AML) system, and the FATF Recommendations have always required the identification of customers and appropriate record-keeping. However, recent developments such as the issuance by the Basel Committee on Banking Supervision of its *Guidance on Customer Due Diligence for Banks*, have shown that the wording of the current Recommendations 10-12 could be developed and refined. The objective is to clarify the obligations to identify and verify the identity of the customer and the beneficial owner, and to perform the necessary due diligence, having regard to current best practice.

5. Section 3.3. deals with three categories of customer or transactions where there is a higher risk: politically exposed persons, correspondent banking and electronic and other non face-to-face financial services. Each part identifies the nature of the risks applicable to the customer or transaction, and suggests options for dealing with those increased risks.

6. In contrast, sections 3.4. and 3.5. set out options that will allow institutions subject to customer due diligence obligations to use simplified or alternative measures for certain lower risk scenarios. Section 3.4. considers whether simplified identification and verification measures could be taken for certain types of transactions e.g. low value insurance contracts, or customers e.g. other financial institutions already subject to anti-money laundering

obligations. Section 3.5. discusses the question of "introduced business" and reliance on third parties to perform certain elements of the customer due diligence process, and suggests a uniform rule for when one could rely on a third party to do this. Finally, section 3.6 identifies a number of other topics relating to customer due diligence, such as section 3.6.1. on whether the identity of customers that held accounts prior to the introduction of the relevant national identification obligation should be verified.

7. Section 3.7. addresses issues concerning suspicious transaction reporting. This is a very important part of every AML regime, and it is now well recognised that financial intelligence units (FIU) have an essential role in the system, and it is proposed that the Recommendations expressly require the creation of such units. Another important issue, which the FATF proposes recognising more explicitly, is the need to provide feedback to reporting institutions. The section also clarifies various issues concerning the nature and scope of the reporting obligation. The final part of this section, s.3.8., examines the standards that the FATF has set regarding the regulation and supervision of institutions from the AML perspective, and suggests various options for clarifying the obligations that apply to regulate and supervise in the FATF context. In particular, the section addresses the steps that countries need to take regarding institutions such as bureaux de change and money remittance companies.

Section 4

8. The FATF has been concerned for several years about the availability of information on the persons that are the true owners and controllers of assets derived from criminal activity, and more recently, various types of 'corporate vehicles' were found to have been used as part of the financing of terrorist activity. The general purpose of section 4 is to address the difficulties that have been consistently identified in FATF typologies exercises in identifying the persons that are the ultimate beneficial owners and controllers of corporate vehicles (companies, trusts, foundations etc.). This information is needed by – (a) law enforcement agencies and FIUs, (b) financial regulators, and (c) financial institutions and other entities subject to AML obligations. An overall consideration for section 4 is that the revised FATF Recommendations will have to reflect a balance in terms of the measures applied to different types of corporate vehicles.

9. Section 4.1. lays out the risks, the obligations that currently apply, the purposes for which beneficial ownership and control information is required, the essential requirements that need to be met, and possible measures that could be taken. There is also considerable reference to *the OECD Report on Misuse of Corporate Vehicles* released in 2001, which lays out three ways in which action could be taken to obtain or have this information accessible. Those alternatives are an up front disclosure regime, the use of company and trust service providers to obtain the information, or reliance on an effective and efficient law enforcement investigative system. The options for action include the need for institutions to perform the necessary customer due diligence measures, and additional commercial law requirements.

10. Section 4.2. examines the issue of bearer shares – these are shares that confer rights of ownership to a company upon the physical holder of the share. They are commonly and legitimately used in a number of countries, but the high level of anonymity may also provide opportunities for misuse in certain circumstances. In particular, there are two money laundering risks: (a) financial assets can be acquired without the purchaser being identified; and (b) companies may be owned and controlled by persons who cannot be identified. The paper also recognises that there are lower risks for bearer shares in companies that are

publicly traded, and that there are substantial arguments suggesting that measures should not be applied to bearer shares in such companies. This section analyses the extent to which bearer shares are a money laundering risk, considers their legitimate uses, and sets out several options for dealing with the risks. The three main options are registration of bearer shares, immobilisation with a custodian, or various systems that allow for the maintenance of information on the beneficial owner of the bearer shareholdings.

11. The transparency of trusts is considered in section 4.3. Trusts are extensively used in many jurisdictions for legitimate personal and business purposes, but in certain circumstances, due to insufficient transparency, the trust may be misused. This section identifies the characteristics of trusts that potentially present risks of money laundering, and propose practical options for eliminating or minimising such risks. Both for trusts and bearer shares, certain minimum standards of transparency are required, and these standards, and options for action are suggested in sections 4.2. and 4.3.

Section 5

12. The current Recommendations recognise that certain types of non-financial businesses and professions are vulnerable to money laundering, and ask countries to consider applying Recommendations 10-21, and 23 to the financial activities of non-financial businesses or professions. However, in recent years FATF Typologies reports have regularly referred to the increasing role played by non-financial businesses and professionals in money laundering schemes. Moreover, the recent amendments to the EU anti-money laundering Directive now apply AML obligations to several additional classes of businesses and professions.

13. In section 5, the FATF thus considers extending the application of the measures contained in Recommendations 10-21 and 26-29 to seven types of non-financial businesses or professions. Those seven categories are:

- Casinos and other gambling businesses;
- Dealers in real estate and high value items;
- Company and trust service providers;
- Lawyers;
- Notaries;
- Accountants and auditors;
- Investment advisors.

14. For each category of business or profession, the paper considers the options for action on several key issues that would be relevant to the application of an AML system: (a) a more precise description of the businesses or professions, and the activities, to be covered; (b) the application of customer due diligence rules; (c) obligations concerning suspicious transaction reporting and increased diligence; and (d) options for regulation and supervision.

15. The FATF wishes to receive the views of all interested parties on the proposals contained in this paper, and non-FATF members, the private sector or any other interested party are invited to provide comments for consideration in the review process. Comments (preferably in English or French) should be received by the FATF Secretariat by 31 August 2002, and if possible they should be sent electronically to: fatf.contact@fatf-gafi.org. Persons providing comments should note that comments received will be made publicly available.

2. INTRODUCTION

2.1. The Forty Recommendations

1. The FATF Forty Recommendations were originally drawn up in 1990 as an initiative to combat the misuse of the financial system by persons laundering drug money. In 1996, based on the experience gained and reflecting the changes that had occurred in the money laundering problem, the application of the Recommendations was extended beyond drug trafficking to serious crimes, and several other changes were made. In addition, a significant number of Interpretative Notes were formulated between 1990-1995, which were intended to provide guidance on more detailed aspects of the Recommendations.

2. The Recommendations have now been endorsed by more than 130 countries, and are widely accepted as the leading international anti-money laundering standard. They are intended to cover all aspects of a national anti-money laundering system, including the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation. They provide an international standard against which many countries from all parts of the world have been assessed through mutual evaluation and self-assessment procedures.

3. It is recognised that countries have diverse legal and financial systems and so cannot all take identical measures. The Recommendations therefore set out the broad standards or principles with respect to which countries must take action. However they do not attempt to prescribe every detail, and providing the minimum standards are met, countries can implement these measures according to their particular circumstances and constitutional frameworks, though each jurisdiction should be able to demonstrate that its anti money laundering regime is effective.

2.2. Background to the Review

4. The principles laid out in the Forty Recommendations have been, or are being, successfully implemented in many countries around the world. However money laundering methods and techniques have changed as new counter-measures are implemented, and there have been other developments that led the FATF to decide during 2001 that it was desirable to commence a review of the FATF Forty Recommendations. The FATF typologies exercises[1], as well as those of FATF-style regional bodies, have shown that money laundering methods, techniques and trends have changed and adapted over time, often as a reaction to the controls and systems that are being implemented to prevent money laundering. FATF members and other countries have noted increasingly sophisticated combinations of techniques, with increased use of legal entities and other corporate vehicles. FATF studies have shown that companies, trusts and other types of business entities are commonly used as part of the laundering process or to disguise the true ownership and control of illegally acquired assets.

5. Another feature of money laundering schemes that has caused increasing concern has been the use of professionals, such as lawyers, notaries, and accountants, by organised crime and other criminals to assist them to launder their funds by acting as financial intermediaries or providing expert advice (so called “gatekeepers”). In many countries, these professionals also specialise in the creation and management of companies and other legal entities or

[1] See http://www.fatf-gafi.org/FATDocs_en.htm#Trends

arrangements, thus providing other services that are useful to the money launderer. It is essential that the Recommendations appropriately deal with these threats. The development of new technologies and on-line financial services may also need to be addressed more specifically in the Recommendations. Although some initial measures were taken by the FATF more than five years ago, the use of such technologies has become far more widespread, and the FATF needs to ensure that the Recommendations cover these and other potential risks.

6. FATF processes for monitoring the implementation of the Forty Recommendations have highlighted a number of areas where the Recommendations need to be strengthened, clarified, or refined. The Non-Cooperative Countries and Territories (NCCT)[2] exercise has also had a significant impact in this respect. The 25 NCCT Criteria which were published in February 2000, and which are used to define non-cooperative countries and territories are based on and consistent with the principles in the Forty Recommendations, though some principles are more explicitly and directly stated. The current review will consider how to incorporate into the Recommendations some of the key details contained in the 25 Criteria, and will provide the mechanism for addressing five "issues of particular concern" identified in the NCCT report issued in June 2000, namely:

(i) The practice in some jurisdictions of an "indirect obligation" to report suspicious transactions related to some criminal offences, whereby making a report provides a defence against a charge of money laundering, rather than a direct obligation to make a report.
(ii) The practice in some jurisdictions of allowing intermediaries to introduce businesses to banks and financial institutions where the obligation to verify customer identity was an obligation for the introducer instead of the bank.
(iii) Difficulties in establishing the beneficial ownership of some legal entities, including companies issuing bearer shares and trusts.
(iv) The existence and development of the International Business Companies (IBCs) which can be formed by intermediaries and be subject to fewer verification and disclosure requirements than applied to the company sector as a whole.
(v) The lack of a stringent scheme to apply the new rules of customer identification for accounts open prior to their entry into force.

7. Since the Forty Recommendations were last amended in 1996, anti-money laundering initiatives have developed both nationally and internationally. At national levels, many countries have taken steps to extend the reach and width of their anti-money laundering legislation and systems, so as to increase their effectiveness. At the regional and international levels, new Conventions or texts have been recently agreed e.g. the United Nations Convention on Transnational Organized Crime and Directive 2001/97/EC of the European Parliament and of the Council, amending Council Directive 91/308/EEC dealing with money laundering ("the EU Directive")[3]. In October 2001, the Basel Committee on Banking Supervision issued its new guidance on Customer Due Diligence for banks[4] ("the Basel CDD

[2] A Glossary of relevant terms and abbreviations is at the end of this consultation paper.
[3] The Directive can be obtained at the following website addresses:
1.http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31991L0308&model=guichett &
2. http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_344/l_34420011228en00760081.pdf
[4] A copy of the paper is available at the following Internet address
http://www.bis.org/publ/bcbs85.htm

paper"). In some cases, these new or amended instruments expand the existing anti-money laundering standards, and the FATF review of the Forty Recommendations is intended to ensure that the Recommendations provide anti-money laundering measures to counter the current threats, and also to anticipate reasonably foreseeable future developments.

8. Another important initiative that occurred in October 2001 was the creation by the FATF of eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organisations, and are complementary to the Forty Recommendations.

9. The Forty Recommendations and Interpretative Notes, the eight Special Recommendations, and the NCCT criteria are collectively referred to as the "FATF framework" within this document. As part of the review exercise the FATF is considering how to ensure that the FATF framework provides a comprehensive and consistent set of measures to prevent and take action against money laundering and the financing of terrorism.

2.3. The Review Process

10. The FATF initially identified a number of areas where possible changes could be made to the FATF framework, and created several working groups to consider certain matters in more detail, while continuing to work at the Plenary level on other issues. The topics or issues which the working groups have considered, and which are set out in detail in Sections 3-5 below, cover issues concerning customer identification, suspicious transaction reporting, beneficial ownership and control of corporate vehicles (including companies, trusts and other legal entities or arrangements), and non-financial businesses and professions (including so-called "gatekeepers"). Each topic identifies the nature of the problem or issue, identifies the risks involved, outlines the current position, and identifies one or more options or alternatives for dealing with the issues or risks. While not explicitly stated for each issue set out below, a further option for many issues might be to retain the current position under the FATF framework. Interested parties should bear this in mind as they read the paper.

11. In addition, the FATF Plenary has continued to work on a number of other areas that are essential and integral to an anti-money laundering system. In particular, further consideration is being given to various aspects of the Recommendations concerning the money laundering offence, the confiscation of the proceeds of crime, and administrative, resourcing and co-ordination issues. International co-operation has been identified as an area needing additional attention, and the FATF is therefore closely scrutinising the relevant recommendations to make sure that effective and efficient co-operation can occur. The review of possible additions and amendments to the FATF framework concerning these issues is subject to ongoing discussion within the FATF, and is not dealt with in this consultation paper.

12. The review process is widely based, and is intended to allow FATF members, FATF-style regional bodies, other international organisations, non-FATF countries and jurisdictions, the financial and other affected sectors, and other interested parties to participate directly in the review process. Moreover, the process is an open one, and any person may provide comments to the FATF on the issues raised in this consultation paper. Following this consultation the FATF will hold meetings with appropriate persons or entities, and then take into account the comments that have been made when preparing more precise proposals for changes to the FATF framework. This consultation will take place both at a national level by FATF members, and by the FATF itself at an international level.

13. FATF members and other countries and territories may send this paper or otherwise make it available to their national associations or groups likely to be affected by the changes, and any other relevant persons or bodies. The FATF encourages those parties providing comments on the issues discussed in this paper to send them electronically to the FATF Secretariat. National associations and groups may also wish to copy their comments to their relevant national authorities. The FATF also requests that where possible, comments are provided in English or French.

14. After 31 August 2002, the FATF will review the comments received, before holding a forum with invited representatives of non-FATF countries and jurisdictions, the financial and other affected sectors, and other interested parties in October 2002 to discuss the proposals for change. All the views received will then be considered when precise changes or additions are made to FATF standards or guidance.

15. In addition to analysing the detailed technical issues, the FATF will also take into account a number of general considerations:

- Avoiding unnecessary duplication of obligations.
- The costs and benefits that arise in relation to particular measures.
- Where possible, ensuring that there be increased consistency, and a "level playing field".
- Generally using a risk based approach when considering the obligations that are imposed.

Although these factors are not listed for each issue below, they will be taken into account when considering the options that could be adopted.

16. The FATF invites comments on the issues and options set out in Sections 3-5 below. Comments are also invited on alternative wording proposals that are set out in square brackets in various parts of the paper. Comments should be received by the FATF Secretariat at the address given on the inside cover **by 31 August 2002**. Persons providing comments should note that comments received will be made publicly available.

3. MEASURES CURRENTLY APPLICABLE TO THE FINANCIAL SECTOR - CUSTOMER DUE DILIGENCE, SUSPICIOUS TRANSACTION REPORTING, AND REGULATION AND SUPERVISION

3.1. Persons or entities to be covered by the FATF 40

3.1.1. Persons or entities engaged in financial activity

17. The FATF considers that it is desirable to describe the "financial institutions" that are currently subject to the FATF framework by reference to an agreed set of financial activities. The term "financial institutions" is widely used throughout the Forty Recommendations and elsewhere, since such institutions are subject to mandatory obligations in many Recommendations. Although the Annex to Recommendation 9 (the Annex) contains a strong indicator of the types of financial activities that are covered, the FATF has not formally defined the term.

18. The FATF considers that the advantage of defining financial institutions by reference to financial activities is that it focuses on what is done rather than on the legal form of entities. This gives more comprehensive coverage than a named-entities approach and minimises the risk of substantial financial activity being outside the scope of the FATF framework. Moreover, continuing with the current approach of leaving "financial institutions" undefined does not provide a robust basis for maintaining the Recommendations as an international standard. However it should be recognised that a consequence of adopting this approach may be that the breadth of the concepts in the definition could require some jurisdictions to extend their anti-money laundering framework to persons or entities that they may not have traditionally considered as financial institutions within the FATF.

19. What types of institutions, businesses or activities are covered by the FATF framework? Most mandatory obligations apply to "financial institutions", which under Recommendation 8 comprise "banks" and "non-bank financial institutions" (NBFI). Although the Recommendation refers to "banks" rather than "credit institutions" (a more general term used in some jurisdictions that also encompasses building societies, credit unions and other deposit taking institutions), it is implicit from the Annex that the financial activities that are covered by the FATF framework include the business of banking i.e. all deposit taking activity.

20. Within the FATF, due to self-assessment and other FATF processes that have focussed on areas of higher risk, the focus has been on certain types of "financial institutions" i.e. banks, insurance companies, stockbrokers, bureaux de change and money remittance businesses. However, while these may be priority areas, the purpose of this paper is to focus on a broader list of functional activities that can be commonly accepted as being those "financial activities" that are at risk of being misused to carry out and/or disguise money laundering and the financing of terrorism.

21. In relation to each functional financial activity, should the FATF framework apply to all persons or entities that carry out that activity? It seems unreasonable to apply an absolute rule whereby the Recommendations must apply to every financial activity, whatever the degree of risk, though this consideration should not lead to the creation of loopholes in the AML framework. Taking into account the factors set out below, the FATF will consider the

parameters within which countries could make a risk-based assessment of the degree to, or manner in which a financial activity should be covered.

22. This issue is already recognised in the language of Recommendation 9, which refers to financial activity that is being conducted as a "commercial undertaking". Therefore, it is proposed that where financial activities are conducted commercially by an entity or person, even though they may be ancillary to their main business, then for the purposes of the FATF framework that entity or person is a "financial institution". But where financial activities are not carried out as a commercial undertaking or are carried out on an occasional basis then the institution is not considered a financial institution for the purposes of the FATF 40.

23. In addition, some consideration needs to be given to the absolute amount of financial activity conducted by the entity. For example, countries could be permitted to "exempt" minor financial activity i.e. below some turnover or activity threshold, from the coverage of the Recommendations e.g. a hotel providing a money changing service where the total turnover is below a threshold and it only conducts transactions for small amounts. This approach is already implied in the Recommendations (see Recommendation 9) and it would also seem to be the practice in some jurisdictions. The advantage of this approach is that it allows jurisdictions to minimise compliance costs for small businesses that are unlikely to pose a significant money laundering risk. The disadvantage is that it potentially encourages criminal elements to focus their illegal financial activities in smaller businesses and it also creates uncertainty about what the international standard is – even allowing some jurisdictions to purposely place significant portions of their financial activity outside of the FATF framework.

24. Using the Annex to Recommendation 9 as a basis for a possible list of "financial activities", FATF is considering adopting a common definition of 'financial institution' as set out in the option below. If FATF adopts this option, this would mean that current Recommendations 10 to 29 (as amended by the proposals in this paper) would apply to all financial institutions:

"For the purposes of these Recommendations, financial institutions means any person or entity who conducts as a commercial undertaking one or more of the following activities or operations[5]:

1. Acceptance of deposits and other repayable funds from the public.[6]
2. Lending.[7]
3. Financial leasing[8]
4. The transmission of money or monetary value, by any means, including by informal channels.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).

[5] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity.

[6] This also captures private banking.

[7] Including inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

[8] This does not extend to financial leasing arrangements in relation to consumer products.

6. Financial guarantees and commitments
7. Trading for own account or for the account of other persons (spot, forward, swaps, futures, options...) in:
   (a) money market instruments (cheques, bills, CDs, derivatives etc.) ;
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.
13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a jurisdiction may decide that the application of anti-money laundering measures is not necessary, either fully or partially."

25. The FATF is also considering how to deal with other situations in which, for particular jurisdictions, there may be minimal risk of money laundering within one or more sectors mentioned above. Certain financial activities and sectors, such as those identified in paragraph 20, have been identified as having greater risks. However, in order to set the parameters referred to in paragraph 21 above, the FATF may consider whether there are circumstances (which would be strictly limited and subject to an overriding consideration that the AML regime must be effective), where countries could simplify certain components of the AML framework.

26. The effect of section 3.1.1. is that the FATF 40 would apply to the entities captured by the definition of financial institution stated above, subject to the considerations mentioned e.g. the amount and frequency of the activity covered, and the consideration mentioned in paragraph 25 above. The FATF seeks comments about:

- The scope of the activities included in the definition of "financial institution" (see paragraph 24).
- The practical consequences for business of applying the Recommendations to entities captured by the definition.

3.1.2. Non-financial businesses and professions

27. The FATF is proposing extending certain mandatory requirements of the FATF 40 to several categories of non-financial businesses and professions that are considered by the FATF to be more vulnerable to money laundering:

a) Casinos and other gambling businesses;
b) Dealers in real estate and high value items;
c) Company and trust service providers;
d) Lawyers;
e) Notaries,
f) Accountants and auditors, and
g) Investment advisors.

Section 5 below contains a detailed consideration of the applicability of the requirements in the FATF 40 to these businesses and professions.

28. In addition, Recommendation 9 currently asks countries to consider applying the FATF 40 to the financial activities of non-financial businesses or professions that might pose a money laundering threat. It is left to each country to determine whether there are additional categories of businesses where a significant money laundering risk is posed for that country. It is proposed that this Recommendation will remain in the FATF 40. Countries should remain vigilant, and could impose anti-money laundering obligations on additional types of businesses or professions that pose a risk.

3.2. The Customer Due Diligence Process

3.2.1. Basic Principles

29. The FATF 40 require financial institutions to identify their customers in certain circumstances, to have verified certain information about their customers and to carry out ongoing scrutiny of the customer relationship. However, the current language of the Recommendations is not clear about the precise obligations that apply. This has resulted in some jurisdictions and institutions interpreting the requirements in such a way that due diligence and record keeping are not always done to a standard that ensures that money laundering investigations can be conducted effectively. The overall objective is for financial institutions to "know their customers" so that the institutions can recognise when financial activity is unusual – and therefore potentially suspicious and/or derived from or intended for use in criminal/terrorist activity - and to have sufficient accurate records available to assist with investigations.

30. The FATF therefore proposes that the FATF 40 specify the distinct elements involved in the customer due diligence process and amend the Recommendations to explicitly set out:

a) What the customer due diligence process comprises;
b) When customer identification and verification needs to be carried out; and
c) What the obligations should be if customer identification and verification cannot be carried out.

Customer Due Diligence process

The Recommendations will explicitly state that financial institutions should:

a) Identify the direct customer i.e. know who the person or legal entity is;
b) Verify the customer's identity using reliable, independent source documents, data or information;
c) Identify beneficial ownership and control - determine which natural person(s) ultimately owns or controls the direct customer, and/or the person on whose behalf a transaction is being conducted[9];
d) Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted - corroborating the information provided in relation to c);
e) Conduct ongoing due diligence and scrutiny - conducting ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, identifying the source of funds.

[9] Please also read section 4 of this document for a discussion on some of the key issues concerning identifying ultimate beneficial ownership of corporate vehicles. Interested parties are invited to comment on any practical difficulties that are foreseen, for example, with respect to particular types of customers or account relationships.

31. Customers, whether usual or occasional, would need to be identified and their identity verified when:

- establishing business relations;
- carrying out occasional transactions above certain thresholds (see section 3.6.3. below);
- making funds transfers; or
- there is a suspicion of money laundering or terrorist financing.

32. It should be noted that the FATF is not proposing that institutions would have to repeatedly identify and then verify the identity of each customer every time that customer conducted a transaction. FATF still considers that an institution is entitled to rely on identification and verification that it has already undertaken unless the institution has doubts about the veracity of that information.

33. Moreover, the FATF is also planning to make the FATF framework more explicit about entities' obligations if they cannot identify or verify the identity of their customers, including the ultimate natural person beneficial owner. Such obligations could include any or all of the following:

a) Prohibiting the entity from establishing business relations with the customer or carrying out any transactions[10].
b) Limiting the activities or transactions able to be conducted through the account e.g. prohibiting the withdrawal of funds from the account.
c) Requiring the entity to file a suspicious transaction report with the FIU.

3.2.2. Integration of FATF standards with those of other bodies

34. The FATF 40 will contain the core minimum requirements relating to customer due diligence issues (i.e. customer identification, verification and on going due diligence). However, the FATF is aware that many of the principles in the FATF 40 need to be supplemented by guidance notes or other clarification to provide sufficient detail for practical implementation.

35. The FATF work on customer due diligence has been proceeding in parallel with work being done by other organisations. The most developed of these other pieces of work has been the publication of the Basel CDD paper.

36. In principle, the FATF is attracted to using the work of other bodies in its revised FATF 40 where their approach is consistent with FATF standards. This has the advantage of avoiding a doubling up of standards or a series of inconsistent standards. The FATF 40 could cross-reference the work of the other bodies as providing relevant guidance for the relevant issues. The alternative is for the FATF to write its own generic guidance for the different types of financial institutions. At this time, the FATF is of the view that the principles in the Basel CDD paper are broadly consistent with FATF standards.

[10] This prohibition might not be applicable where the entity has been asked by competent law enforcement or regulatory authorities to continue with the relationship or transaction for monitoring purposes.

37. Accordingly, the FATF believes that, in principle, paragraphs 18 to 59 of the Basel CDD paper could apply to all financial institutions if they are carrying out the type of activity covered in the relevant paragraph(s) of that paper e.g. if the financial institution does not carry out correspondent banking then the paragraphs on correspondent banking in the Basel CDD paper are not applicable. Moreover, if the Basel CDD paper is to be applicable beyond banks, some of the concepts in the paper may need to be applied generically instead of just to banking. For example, references to opening accounts could be read as opening or commencing relationships, and references to correspondent banking might be read as references to correspondent relationships.

38. However, the FATF also notes that the Basel CDD paper was developed primarily for banks. Some of the approaches might not be fully suited to other financial institutions given the nature of the different industries in the financial sector and the money laundering threats that exist.

39. One area where this could be the case is the securities industry. For example, in that industry not all securities dealers operate client accounts; securities markets operate rapidly in many jurisdictions, which could affect the account opening process; and the funds may already be in the financial system.

40. The FATF is particularly interested to hear from the non-bank financial sector about the practical difficulties of requiring them to follow the minimum standards in the Basel CDD paper when carrying out customer due diligence. The FATF is interested in this consultation to hear what further modifications, in addition to those outlined in this discussion paper, the non-bank financial sector would require in order to make the proposals workable without compromising FATF objectives of making money laundering and the financing of terrorism difficult to carry out and providing authorities with a reliable and accurate transaction records.

41. In considering this issue financial institutions should take into account the full range of proposals that the FATF is consulting about. In particular, sections 3.4 and 3.5 contain discussions about situations where institutions might be able to carry out simplified due diligence on their customers and to rely on third parties to carry out some of the due diligence process.

3.3. Higher risk customers or transactions

3.3.1. Politically Exposed Persons

42. Corruption and abuse of public funds by some government leaders and public sector officials - often collectively referred to as Politically Exposed Persons (PEPs) – has become a subject of growing concern, internationally and in individual countries, in the last couple of years. Several high-profile investigations (e.g., Abacha, Montesinos, Marcos) have highlighted not only the enormous scale of illegal wealth acquired by some corrupt leaders and officials but also that the proceeds of corruption are typically transferred to a number of foreign jurisdictions and concealed through private companies, trusts or foundations, or under the names of relatives and close associates of the PEP.

43. There are various concerns. Corrupt acquisition of state assets or wealth causes damage, both social and financial, to the countries concerned, many of which are relatively poor. At the same time, there is increasing awareness of the risks posed to banks and financial systems that handle the proceeds of corruption or abuse of public funds. In accepting and handling funds from such sources, financial institutions must recognise the implications, which include: reputational damage; restitution claims from national governments or private individuals; significant legal and compliance costs; enforcement action by the regulatory authority; and criminal charges of money laundering against employees of the financial institution or the institution itself. Furthermore, to the extent that the proceeds of corruption are routed through a number of firms in the same financial centre, then that centre may itself suffer reputational damage and loss of public confidence in its business standards.

44. There seem to be two schools of thought on the issue of PEPs. On the one hand, it is argued that no special guidance to financial institutions is needed in respect of handling accounts linked to PEPs. If customer due diligence procedures are properly applied at the account opening stage, and transactions through PEP accounts duly monitored against what is known of the customer's legitimate business or personal activities, then corruption or misuse of public funds should be readily picked up and reported to the criminal authorities. In broad terms, the argument continues, PEPs as a topic is part of a general risk management framework, albeit an important part.

45. On the other hand, it is arguable that PEPs are different from other categories of customer, for the reasons referred to above and because of the high public profile (notably in the Abacha case) when failings were found to have occurred.

46. The authorities of three FATF jurisdictions have issued relevant guidance to their financial institutions. There now appears to be a growing consensus that PEP guidance should be part of a wider international agenda for action. Some work on appropriate guidance has recently been undertaken informally by a group of supervisors from several countries, which could form the basis for setting appropriate international standards or guidance. This guidance embodies the following broad sub-headings:

- definition of a PEP;
- identifying PEPs during account opening;
- decision to open an account for a PEP;
- enhanced diligence in monitoring PEP accounts; and

- review of ordinary accounts in order to identify PEPs.

47. The first issue to decide is whether an explicit reference to PEPs is necessary or desirable in the revised FATF 40. It is worth noting that the Basel CDD paper dealt with the issue specifically – see section 2.2.5 of the Basel CDD paper. If it is necessary, how could this best be done?

- **Option 1** would be to have a general statement in the Recommendations about minimum standards applicable to all account relationships, followed by a reference to the need for higher standards in certain high-risk areas like correspondent banking and PEPs. This might be considered enough on its own.

- **Option 2** would be to supplement the first option with a cross-reference to the Basel CDD paper. However, a legitimate question is whether the Basel text, albeit an excellent summary of the risks, provides sufficiently detailed guidance to stand on its own.

- **Option 3** would be to include some concise text within the FATF 40, possibly as part of a new 'Customer Due Diligence' Recommendation. That could cross-refer to a much more detailed guidance paper that would include a variety of detailed 'CDD' issues – including correspondent banking, reliance on third parties to perform identification functions, etc.

3.3.2. Correspondent Banking

48. The FATF considers that correspondent banking is an area where the higher risks of money laundering and terrorist financing mean that it needs to be treated differently from other business relationships involving two or more financial institutions (see Section 3.4 below). Recent studies of the financial aspects of terrorism and of money laundering have highlighted the need for enhanced due diligence on the part of banks that provide correspondent accounts, particularly to banks in other countries. This paper draws on a variety of source material to:

- explain what correspondent banking is;
- outline the money laundering risks posed;
- set out key elements of best practice to counter those risks, based on guidance in the Basel CDD Paper and in three FATF members; and
- set out some options for dealing with the issue within the Recommendations.

49. The reference in this section is to "correspondent banking". However, as mentioned previously, the FATF is also considering whether this section should be broadened to deal with all correspondent relationships between financial institutions e.g. similar relationships in the securities industry.

3.3.2.1. What is Correspondent Banking?

50. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). By establishing multiple

correspondent relationships world-wide, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for hundreds of other banks around the world. Respondent banks are provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers of funds, cheque clearing, payable-through accounts and foreign exchange services. The services offered by a correspondent bank to smaller, less well known banks may be restricted to non-credit, cash management services. But those respondent banks judged to be sound credit risks may be offered a number of credit-related products (e.g., letters of credit and merchant accounts for credit card transactions).

3.3.2.2. The money laundering risks posed

51. Correspondent banking lies at the heart of the international payment system, allowing banks world-wide to make payments to and through each other. The effective working of the international payment system depends upon three principal attributes: speed, accuracy and geographic reach. But these attributes may also create considerable vulnerability to money laundering. The sheer volume of payments, added to the speed at which they must move, make it very difficult to identify and intercept payments unless both the originator and the recipient are identified to the handling bank as problematic in advance and are clearly identified in the transmittal information. Once criminal funds have entered the payment system, it is extremely difficult to identify those funds as they move from bank to bank.

52. The correspondent bank therefore continually provides services to, and receives funds on behalf of, customers of the respondent bank – with whom it often has no direct relations and does not know. This is a situation that criminals can, and do (as has been well documented), exploit. The FATF Typologies report issued in February 2002 found that correspondent banking relationships have certain vulnerabilities that, if left unchecked, may be exploited by criminals that are seeking access to the financial sector, while also seeking to conceal their identities or the true nature of their activities. There was especial concern where a respondent bank serves as a correspondent for other financial institutions, and a number of case examples are cited in that report.

3.3.2.3. Failures of due diligence

53. The types of weaknesses that have been found in banks' ongoing anti-money laundering oversight of their correspondent accounts are as follows:

a) Failure to ask respondent banks about the extent to which those respondents allowed other banks to use their accounts with the correspondent bank. In this way, the correspondent bank might find itself indirectly conducting business for a number of offshore or shell banks with which it would not even consider establishing a direct account relationship.
b) Variable degrees of due diligence on correspondent relationships, depending on whether credit was being granted. Extension of credit facilities necessitated an evaluation of the foreign bank's management, finances, business activities, reputation, regulatory environment and operating procedures. But for fee-based services, e.g., wire transfers or cheque clearing, the same degree of due diligence was often not undertaken. Since the highest-risk foreign banks were rarely extended credit, they often seemed to avoid banks' anti-money laundering systems and

controls. Moreover, some correspondent banks did not always undertake periodic reviews of their relationships with respondent banks, even when there had been negative press reports about a particular bank, which if they had been reviewed, may have triggered a fundamental review.

3.3.2.4. Key elements of best practice to counter money laundering risks

54. From the evidence of money laundering 'typologies', and from the guidance issued in several countries to their banks, there seem to be certain key requirements to counter money laundering risk through correspondent banking facilities:-

- Institutions should refuse to enter into, or continue, a correspondent banking relationship with a respondent in a jurisdiction where it has no physical presence (a so-called "shell bank") and which is unaffiliated with a regulated financial group. Banks should also guard against establishing relations with respondent foreign institutions that permit their accounts to be used by shell banks.

- Institutions should not enter into correspondent relationships unless the correspondent and the respondent have documented and agreed to their respective roles in respect of anti-money laundering obligations in the framework of the legal obligations that apply to the entities concerned.

- Institutions should not enter into any correspondent relationship unless satisfied that they have received all the necessary information, and have been able to conduct appropriate due diligence. As a minimum, in order to allow proper risk assessment and decision-making, due diligence should consist of:

  - Collecting information about the respondent's ownership, management, major business activities, where it is located, the quality of its money laundering prevention and detection efforts and whether the respondent maintains accounts with other correspondent institutions in the same jurisdiction.
  - Collecting information on the volume and nature of the transactions expected to flow through the correspondent account and whether the respondent allows other institutions to use their accounts with the correspondent institution (if so, which other institutions).
  - Considering the rigour of supervision in the respondent's home jurisdiction.

- Taking appropriate measures to deal with the risks associated with "payable-through" accounts or any other type of account where sub-account holders are allowed direct access to a correspondent account. Options for dealing with such risks include:

  - Prohibiting the provision of such "payable-through" facilities.
  - Performing full customer due diligence procedures on the sub-account holders. The obligation to perform these procedures could be placed on –
    (i) the correspondent institution to identify all the sub-account holders using its correspondent account, or
    (ii) the respondent institution to verify the identity of and perform on-going due diligence on the customers it allows to operate the payable-through facilities and

to [provide copies of] [make available] the identification records to the correspondent.
(iii) the correspondent institution to ensure that they either know who the sub-account holders are or that they are certain that the other bank is performing adequate due diligence and that they can test for that information, obtain it and rely upon it.

- Institutions should train their staff dealing with correspondent accounts to recognise higher risk circumstances or irregular activity, whether isolated transactions or trends, and submit a suspicion report where appropriate.

- Institutions should conduct periodic reviews of all their correspondent account relationships to identify higher risk respondents and close accounts with problem institutions.

55. Additional due diligence policies and procedures may need to be applied in certain circumstances of increased risk, e.g., where a particular jurisdiction has been identified by FATF as "non co-operative" in the fight against money laundering or is linked with terrorist financing. These procedures might include:

- reviewing publicly available information to determine whether the respondent institution has been the subject of a money laundering or other criminal investigation or any regulatory enforcement action for breaches of anti-money laundering regulations;
- discussing the respondent institution's anti-money laundering controls with senior management of that institution;
- requiring the correspondent institution's senior management to approve any continuation of the account relationship.

56. Neither the Recommendations themselves, nor any of the Interpretative Notes, refer explicitly to the risk of laundering through correspondent banking relationships. However, there are clearly identifiable risks, particularly for large banks conducting operations world-wide. Furthermore, the Basel Committee regarded the subject as important and provides guidance on the issue in its CDD paper. So the inclusion of an explicit reference to correspondent banking in the revised FATF framework is both necessary and timely.

3.3.2.5. Options for Action

57. The FATF has identified two alternative ways of dealing with the issues outlined above:

Option 1 would be to have a general statement in the Recommendations about the minimum standards applicable to all account relationships, followed by a reference to the need for higher standards in certain higher-risk areas like correspondent relationships and politically exposed persons. There should also be a cross-reference to the relevant parts of the Basel CDD paper. If this option were adopted, it may also be desirable to draw out and emphasise certain key elements from the Basel text, such as the prohibition on establishing correspondent accounts for a respondent institution that has no physical presence in any jurisdiction (a shell bank), except where that institution is affiliated with an adequately regulated financial group.

Option 2 would be to include some concise mandatory text within the Recommendations, possibly via a new 'Customer Due Diligence' Recommendation. The main elements of that mandatory text would be:

- the basic principle that the correspondent institution remains ultimately accountable for all financial activity that occurs through its correspondent accounts; and
- the key requirements set out in the Basel CDD paper and in paragraph 54 above. This text could either stand alone or could be supplemented by a more detailed guidance paper based on the above paragraphs. That guidance would also encompass other more detailed aspects of customer due diligence issues, such as politically exposed persons, eligible introducers, etc.

Comments are also invited on whether additional controls and due diligence should be applied to relationships between other types of financial institutions that are similar in nature to correspondent banking relationships.

3.3.3. Electronic and other Non Face-to-Face financial services

58. The financial sector is continuously evolving and responding to customer demand for better, more flexible and faster services. Combined with technological developments this has led to the provision of more financial services and transactions over the Internet and through using other methods where there is little or no face-to-face contact between staff of financial institutions and their customers. Other non-face-to-face methods include the use of ATM machines, telephone banking, the transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transactions using prepaid or reloadable or account linked value cards. It is common in many jurisdictions for customers that use these types of services to conduct most of their regular "banking" business without any physical contact with the staff of the financial institution. These developments are enhancing customer service and economic efficiency. However, they may also provide money launderers with additional opportunities that financial institutions and authorities need to address.

59. The FATF 40 contain only a brief reference to these issues. Recommendation 13, while not specifically referencing non face-to-face financial services calls on jurisdictions to pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

60. Consideration needs to be given to the nature of the potentially higher money laundering risk associated with electronic and non face-to-face financial services and transactions. The FATF will then determine whether the FATF 40 should be extended to address this specific risk, perhaps by setting out guidance or minimum standards for customer interaction where customers can conduct transactions without the need for formal scrutiny or clearance by staff members in financial institutions.

61. In other fora, the recently amended EU Directive, as modified, confirms the necessity for financial institutions and other persons, to take specific and adequate measures necessary

to compensate for the greater risk of money laundering which arises when establishing business relations or entering into a transaction with a non-face-to-face customer. Such measures are designed to ensure that the customer's identity is established, for example by requiring additional documentary evidence, or by other supplementary measures. Moreover, the Basel CDD paper provides general guidelines that are intended to ensure that banks apply customer identification procedures and on-going monitoring standards for electronic and other non-face-to-face customers that are equally effective as those for other customers.

3.3.3.1. Risks

Opening accounts and establishing customer relationships

62. All business relationships for financial services that are established without face-to-face contact between the staff of a financial institution and the customer present risks. This is the case whether an account is opened via the Internet or the receipt of an application form from a prospectus via the post. Even though the problems concerning the verification of the identity of the customer are of the same nature as in traditional financial institutions, the dematerialization of the procedure for establishing the relationship intensifies the difficulties involved. Thus "Internet institutions" may attract non-resident customers wanting to take advantage of the potential lack of transparency in automated transaction processing and other aspects of non face-to-face financial services.

63. There appears to be a general consensus that on-line financial services per se do not present new specific risks of money laundering, beyond the risks applicable to all non-face-to-face relationships, provided full due diligence checks are applied. Yet, there are three main factors that may aggravate more typical risks for on-line accounts:

- ease of access to the network, regardless of location, equipment or time of day;
- dematerialization; and
- the rapidity of electronic transactions.

These three factors, along with automation of financial operations may make due diligence more difficult to perform.

3.3.3.2. Dematerialization and automation of operations

64. Financial services provided over the Internet have the potential to result in the relationship between a financial institution and its customer being conducted without appropriate due diligence because of the automation (and dematerialization) of interactions. This potential risk should be addressed by the use of effective online or other identification procedures applicable to these services..

65. The money laundering risks are also potentially greater because there is no personal relationship between a customer and financial institution staff. The FATF understands that Internet based financial institutions have significant customer numbers, but with fewer compliance staff than in traditional bricks and mortar institutions. The FATF seeks comments on whether this is the case and on how Internet based institutions can ensure that they are able to know their customers, and have an effective monitoring system.

3.3.3.3. Non-cash transactions/transfers

66. Listed below are examples of non face-to-face transactions for which additional risks may arise. The FATF is seeking comment on whether additional guidance is necessary to mitigate some or all of these risks:

- Cash withdrawals and deposits using ATMs and electronic point of sale terminals usually occur without any face-to-face contact between customers and institutions, and may result in institutions having greater difficulty in conducting appropriate due diligence.
- Customers can transfer funds between accounts or effect payments without any face-to-face interaction, which may make it more difficult for institutions to identify suspicious transactions.
- Automated processing of transfer orders prevents financial institution staff checking the order in advance with respect to the account activity pattern, the destination of the funds and the account holder's income, business activity and residency status.
- Straight through processing often involves cross-border transfer of funds. The different payment systems currently in use and the lack of standardised message formatting may make effective monitoring of such transactions more difficult.

3.3.3.4. Electronic money (purses and cards)

67. The term electronic money designates a claim on the issuer of the money that is stored in an electronic medium and is accepted as payment by third parties other than the issuer. The electronic medium could be a smart card, in which case it is called an electronic purse. When the medium is a server run by the issuer and is accessible through the Internet from PCs running the appropriate software, it is referred to as a virtual purse.

Electronic purses

68. FATF Typologies reports have suggested that the risk of money laundering for electronic purses is greater if the device preserves the user's anonymity and makes it possible to transfer funds from one card to another.

69. Electronic purses can be loaded with stored value directly from an account over the Internet or else by buying value with an ordinary bank/institution card. Many systems also offer to handle on-line payments to virtual merchants. These payments are made using a smart card reader hooked up to a PC or even a mobile phone. They do not create any risks other than those that have already been identified in the case of conventional use of electronic purses. These purses, if they are anonymous and have the capacity to transfer funds to another card, could be used for money laundering, since they make it possible to dissipate income or transfer funds. Measures that could mitigate the potentially higher risk include setting limits on the amount that can be stored on a card, the number of times a card can be recharged, and the number of cards each customer is allowed to hold. Some promoters of electronic purses have adopted some of these restrictive characteristics at their own initiative.

70. Some regulators believe that people should be identified when they receive electronic purses with a stored value capacity over a certain amount and/or when they acquire or re-load electronic money in excess of a certain amount by means other than debiting an account held with a financial institution that is subject to customer due diligence requirements.

Virtual purses

71. Virtual purses hold a reserve of value in a personal computer in order to purchase on-line services. The risk of money launderers' making use of virtual purses arises because the reserve of value can be used anonymously to acquire assets (particularly financial assets) or to transfer funds.

72. The risk appears to be limited, however, since the reserve of value is usually created and maintained by withdrawals from an account with a financial institution and the number of a bank/institution card must usually be produced to move funds to the reserve. However this may only mean that the transaction can be traced, and may not guarantee that the holder of the account has been identified. It is even possible that a virtual purse could be created or maintained using an electronic purse that is itself anonymous.

73. Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money requires that suppliers of virtual purses and electronic purses in EU jurisdictions must be institutions that are subject to customer due diligence and suspicious reporting requirements as provided for by the EU Directive.

74. Another factor that potentially mitigates the risk of money laundering is the maximum capacity that is usually applied to virtual purses, which limits the nature and the amount of the transactions for which it can be used. Currently, any such limits are usually established by purse/card issuers.

75. Finally, there is always a risk of other services being developed for virtual purse owners, in addition to the dedicated payment service currently offered. Such services could turn virtual purses into truly anonymous accounts with all the money laundering risks that anonymity provides.

3.3.3.5. The potential impact of Internet-driven competition on customer risk management

76. Listed below are some potential concerns that may be an unwanted by-product of Internet driven competition. The FATF is seeking comment on whether additional guidance is necessary to mitigate these possible risks:

- An Internet financial institution's risk management system may be compromised either by the firm's decision to favour immediate returns or by an unexpected surge in the volume of customer risks that could overwhelm a small firm.
- New, internet-only financial institutions could lack the tradition of risk awareness associated with experienced firms.

3.3.3.6. Options

77. There are several options that the FATF could take to deal with the issues outlined above.

- **Option 1** - to amend the FATF 40 to emphasise that there are increased risks when carrying out non-face-to-face transactions and that countries are required to adopt adequate measures to counter such risks, without listing such measures. This approach was adopted in the EU Directive. Such an approach has the advantage of allowing countries flexibility when deciding on the most appropriate controls, and is also flexible enough to deal with future technological change. However, the disadvantage of this approach is that there is no statement about what measures are "adequate".

- **Option 2** - to amend the FATF 40 to include a requirement that jurisdictions put in place measures to mitigate the increased risk of money laundering (i.e. Option (1)), and provide a list of measures which may alleviate these risks. Such measures would not be mandatory or exhaustive. (A list of possible measures is discussed in Annex 1). Jurisdictions would be expected to adopt at least some of the measures recommended as well as to demonstrate in any mutual evaluation or assessment process that these measures represent an adequate response to the risk of money laundering. This is the approach adopted in the Basel CDD paper. However, if these additional measures do not provide a reliable method for non face-to-face identification, the normal customer due diligence requirements would apply.

- **Option 3** - to amend the FATF 40 to specify a list of "adequate" measures (i.e. Option (2)) and require countries to select at least several measures from the approved list. Countries would have discretion to include further supplementary measures if they so choose. Such an approach has the advantage of allowing countries some flexibility in order to meet the specific characteristics of their market while creating a level playing field for participants. However, if these additional measures do not provide a reliable method for non face-to-face identification, the normal customer due diligence requirements would apply.

Whichever option is finally adopted, financial institutions may also need to pay particular attention to the bona fides of Internet institutions that engage in financial activity to ensure that they are reputable and subject to any applicable international supervisory standards. This is because of the risk that some may be operating in a supervisory or regulatory "vacuum".

3.4. Simplified due diligence procedures

78. The wording of FATF Recommendations 10 and 11 imposes an obligation on financial institutions to identify their clients. They do not contain any reference to situations where financial institutions would not be required to identify their customers or where reduced or simplified requirements could be implemented. However in practice, many jurisdictions have defined particular circumstances under which the normal customer due diligence requirements are not applicable. The FATF is therefore giving consideration to defining the situations in which, having regard to the money laundering risks and other relevant factors, it would be reasonable to let jurisdictions decide that their financial institutions need not be subject to the normal identification obligations, and for identification not to be verified or recorded, or that more limited obligations could apply. However, the application of simplified procedures would only be allowed in the limited circumstances outlined in this section, and should not undermine the key due diligence principles stated above. Moreover, simplified procedures should be differentiated from the circumstances in which it would be reasonable for a financial institution to rely on a third party to perform most of the elements of the identification function, and to provide appropriate records to the institution (*see section 3.5 below*).

79. When using the term customer due diligence in the context of the FATF framework, as noted at paragraph 30 above, it must be remembered that this actually involves several distinct elements or stages in a process, and that these differences can be important for specific issues. When considering the circumstances in which simplified procedures could be applied, the relevant stages are identifying the customer and any "beneficial owner" and verifying their respective identities i.e. :

a) identify the direct customer;
b) verify the customer's identity;
c) identify the person with beneficial ownership and control;
d) verify the identity of the beneficial owner and/or the person on whose behalf a transaction is being conducted);
e) conduct ongoing due diligence and scrutiny.

As previously mentioned, the FATF framework will be re-written in a way that ensures that these separate stages are explicitly identified.

80. There are also certain other 'checks and controls' that are often implemented as a matter of practice, and regardless of any laws. For example, financial institutions usually identify their customer (element (a) above) for business reasons; and in many jurisdictions, financial regulators perform extensive checks on the identity of certain types of financial institutions, their owners/shareholders and senior management, as part of licensing procedures. These additional checks may provide some level of comfort for financial institutions.

81. When considering the issues raised herein, a number of general principles will continue to apply, regardless of specific situations where there are simplified requirements. The starting point should always be the general rule that all customers (including beneficial owners or controllers) must be fully identified and that this is verified. Any use of simplified procedures should be strictly limited. Secondly, simplified procedures should not apply to transactions or relationships that appear to be intended to avoid identification obligations, or are otherwise suspicious.

3.4.1. Circumstances in which Identification and Verification obligations are either simplified or do not apply

3.4.1.1. Particular types of transactions

82. Most EU member states have allowed financial institutions certain concessions with respect to the identifying and/or verifying the identity of their permanent customers (as opposed to one-off occasional customers[11]). These concessions, which are based on the EU Directive, allow EU member states to waive the customer identification and/or verification requirements for institutions in the following circumstances:

a) entering into life insurance policies with an annual premium of no more than €1000, or a single premium of no more than €2500;
b) entering into insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

83. The circumstances outlined in paragraph 82(a) & (b) above are lower risk, and it is reasonable to consider making an express reference to these types of exemptions within the FATF framework, although the concession should not apply if money laundering or structuring[12] is suspected, as outlined in section 3.6.3. below.

3.4.1.2. Particular types of customers

84. Article 3(9) of the Directive provides that identification/verification requirements do not apply in certain circumstances where the customer is a credit or financial institution:

> *"9. The institutions and persons subject to this Directive shall not be subject to the identification requirements provided for in this Article where the customer is a credit or financial institution covered by this Directive or a credit or financial institution situated in a third country which imposes, in the opinion of the relevant Member States, equivalent requirements to those laid down by this Directive."*

85. This has been implemented by most EU jurisdictions, though in slightly varying ways. In addition, some other FATF jurisdictions have also allowed their institutions to have simplified requirements when identifying certain categories of customer: (a) larger public companies listed on a stock exchange, (b) where the identity of the contracting partner is publicly known[13], and (c) state administrations or enterprises. A summary of the current position regarding all types of customers in FATF member states is set out at Annex 2.

86. Even where the customer is a credit or financial institution, although there may be simplified requirements concerning certain elements of the identification process, this does

[11] Occasional customers are generally not subject to identification obligations unless the relevant transaction (or a series of linked transactions) exceeds a defined threshold. Under the EU Directive this threshold is €15,000.

[12] Structuring refers to situations where cash transactions above a certain threshold may result in customer identification or reporting requirements. The launderer then conducts several transactions below the threshold rather than a single transaction above it, in an effort to avoid these requirements.

[13] In one FATF country, the identity of a legal entity is deemed publicly known if it is a public company or associated directly or indirectly with a public company.

not in practice mean that none of the elements of the customer due diligence process are performed. Accounts held for institutions are either used to conduct transactions for the customer institution itself or perhaps more frequently for the customers of that institution (for example, the use of a correspondent banking account[14], or an account that pools the funds of clients of the customer institution for investment purposes). The key issue therefore is whether the institution holding the account should be subject to identification obligations concerning (a) the customer institution and (b) the clients of the customer institution.

(a) Concerning the customer institution itself, in practice its identity would be checked through independent sources, to confirm that it is a credit or financial institution. This would normally be done by checking certain reliable lists of authorised financial institutions (often such lists are maintained on the website of the supervisory authority), or by confirming with the relevant supervisory authority that it is a licensed/registered institution. Such checks would probably not normally encompass checks on the beneficial owners of that institution, though the fact that the customer is an authorised institution will often provide sufficient comfort by itself.

(b) As regards the clients of the customer institution, most jurisdictions set out specific and defined circumstances in which it is reasonable for the institution holding the account to rely on the customer institution to identify and do due diligence on its own clients. There are a number of situations in which this would appear reasonable, e.g. where an account is used to pool investment funds from many clients for transparently legitimate purposes.

87. Two issues arise which merit further consideration. The first concerns which countries or jurisdictions can be said to have anti-money laundering measures that meet the standards in the FATF framework, and thus it might be reasonable to rely on credit or financial institutions from that jurisdiction. This question is discussed elsewhere, since the same or a very similar issue arises with respect to reliance on third parties to perform identification functions (see Section 3.5.3.1 (Third parties from which jurisdictions) below).

88. The second issue is whether it is reasonable to not perform full identification/verification checks on all types of financial institutions, since this encompasses a potentially wide range of institutions, some of which may not be subject to the same type of supervision as banks or securities firms. These concerns have been recognised in some EU states, where it is a requirement that the institution must also be fully regulated or supervised. Thus, institutions such as bureaux de change, which may not be fully regulated or supervised in some countries, are subject to all the normal requirements. This is part of the wider issue concerning the types of institutions or entities that need not undergo the full identification process. As noted above, publicly listed companies and state administrations or enterprises do not need to be identified in some FATF members.

89. In considering what approach the FATF might take, consideration should be given to the reasons why reduced identification requirements for certain types of institutions or companies could be appropriate, and to the risks that might arise from creating these

[14] Note the proposals set out at section 3.3.2. for increased due diligence in respect of establishing and maintaining correspondent relationships between institutions. These proposals apply in priority to the issues discussed in this section of the paper.

exceptions to the normal rule. Reasons for not applying full identification/verification obligations (including obligations to identify the beneficial owner) might be that:

- it is easier to identify the customer and verify their identity due to information that is publicly available e.g. a large, publicly listed company.
- existing checks and controls elsewhere in the system are adequate to meet the identification obligations, e.g. the customer institution itself is subject to effective anti-money laundering requirements and regulatory supervision, and identifies its own customers and records that information.
- the cost burdens would be high, and the risks low if identification measures had to be applied to relationships and transactions between credit and financial institutions. It might also be argued that this would result in extensive duplication of identification requirements.

90. These rationales should be contrasted with the potentially increased risk that the institution is owned or controlled by criminal elements and is therefore knowingly involved in money laundering activity. This risk may be small for large publicly traded or regulated institutions, but could be greater for smaller less closely regulated institutions, e.g. certain bureaux de change or money remittance businesses. Risks also increase where the customer institution or entity operates the account for its own customers. For example, payable through accounts or correspondent banking relationships often involve transactions for the clients of customer institutions (or even the clients of clients). This may involve an increased risk of layers of transactions and the lack of identification of the person on whose behalf the transaction is ultimately being conducted.

91. A majority of FATF members have systems that allow their institutions subject to anti-money laundering measures certain concessions from the normal full identification and verification obligations. It is also reasonable to assume that explicit recognition of appropriately defined concessions to the normal rule could increase consistency, eliminate potential loopholes that might occur through different rules in different countries and reduce potential regulatory arbitrage. It is also likely that this might make the legal or regulatory obligations closer to regulatory and business realities in many members. It is therefore proposed that the FATF framework should explicitly state that countries may provide for certain situations where the normal identification/verification obligations mentioned in paragraph 30 can be relaxed or simplified, but only within the parameters discussed below.

Options

92. The options for permitting simplified requirements could apply to the following types of customers, provided that the account holding institution is satisfied that the customer institution or entity meets the necessary criteria. However in all cases, if specific higher risk scenarios apply, e.g. requirements concerning correspondent accounts (see section 3.2.), then the simplified requirements would not apply.

Simplified due diligence procedures could apply to the following types of customers, provided that they meet the necessary criteria:

Option 1
Banks or credit institutions only – on the basis that in most countries there are reasonably detailed licensing processes, the full range of anti-money laundering obligations apply, and they are supervised.

Option 2
Credit and financial institutions (in line with the EU Directive). These institutions are all subject to the FATF framework, and thus should be identifying their customers. However, there may be a case for restricting this exception to those types of institutions that competent authorities ensure are complying with the FATF requirements.

Option 3
All institutions or entities that are subject to the full range of anti-money laundering obligations that are applied in accordance with the FATF framework.

There could also be certain other options available to jurisdictions in circumstances where money laundering risks may be lower because of the availability of public information on the ownership of the customer entity or the nature of the ownership:

Option 4
Some categories of large companies where information about their ownership is readily available e.g. publicly listed companies.

Option 5
State/government owned entities and other public bodies.

93. Each jurisdiction could also decide whether to apply the exceptions only to entities in its own jurisdiction or extend the exceptions to entities from any other jurisdiction that the original jurisdiction is satisfied applies anti-money laundering requirements in accordance with the FATF framework. [see discussion on jurisdictions with equivalent anti-money laundering measures in Section 3.5.3.1. below]

94. As regards the normal obligation to identify the beneficial owner or controller of an account held by another financial institution, or the person on whose behalf a transaction is conducted, it must be recognised that there a number of situations in which it would be unreasonable to require the identification and record-keeping processes to be duplicated in several institutions. This is recognised in the Basel CDD paper, which provides specific guidance on a number of scenarios where an account holding institution can rely on the customer financial institution to perform the customer due diligence on the beneficial owner, and on the specific measures that the institution must take to ensure that such reliance is acceptable (for example see section 2.2.4 of the Basel CDD paper). Similar guidance has been or is being developed for the insurance and securities sectors.

95. It would not be appropriate for the FATF to enumerate in the Recommendations all the circumstances and the special conditions in which an account holding institution should or

should not rely on a customer financial institution to perform due diligence on its clients. The most viable option would therefore seem to be to indicate in the Recommendations that:

> There are limited circumstances in which it is reasonable for the account holding institution to rely on the customer financial institution to perform due diligence on its clients, and:
>
> **Option 1**
> The circumstances are outlined in the Basel CDD paper (section 2.2.4).
>
> **Option 2**
> The circumstances will be outlined in FATF guidance on customer due diligence issues (which will be prepared in the future).

3.5. Reliance on third parties to perform Identification and Verification obligations

96. The NCCT exercise identified the issue of "eligible introducers" (paragraph 60(i) NCCT report June 2000) as an issue of particular concern that should be considered as part of the review of the Recommendations. The issue was defined as "The practice in some jurisdictions of allowing intermediaries to introduce businesses to banks and financial institutions where the obligation to verify customer identity was an obligation for the introducer instead of the bank".

97. The issue of "eligible introducers" is part of a wider issue, namely, the financial institution accepting the customer and relying on third parties to perform certain elements of the due diligence process concerning identifying customers and verifying identity. In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another financial institution or third party, e.g. a lawyer in the same or another jurisdiction. It may also occur in business relationships between insurance companies and insurance brokers/agents, or between mortgage providers and brokers. Common examples of where a third party could be involved are:

- A customer of a bank applies to buy an investment product (e.g. term deposit or units in a unit trust) with another financial institution. Payment is made using the customer's cheque drawn on the first bank. The second institution relies on the identification and verification of the customer done by the first bank. At maturity of the investment product, the second institution, acting on the customer's instruction, pays the funds to a securities broker. The securities broker relies on the identification and verification done in the other financial institutions – essentially the original bank.

- A customer places funds with a bank, which carries out the required due diligence. The customer wishes to set up a trust into which to place some or all of their assets, and the bank introduces the customer to a trust service provider (TSP); (probably a group company but not necessarily). The TSP may provide the trustees and in administering the trust may invest some of the funds in a mutual fund or purchase an insurance policy. Reliance can be placed by the TSP, the fund manager and the insurer on the due diligence carried out by the bank, if the conditions for an introducer have been met.

- Independent investment advisors provide an intermediary financial services role in a number of countries. Such an advisor may introduce a client to an insurance company for the purpose of taking out a life insurance product, and also perform the identification and verification functions, before passing the necessary documentation to the insurance company.

- In the securities sector, brokers in one jurisdiction may often purchase shares at the request of a foreign broker for the client of the foreign broker. In many countries, the domestic broker would rely on the foreign broker to perform any necessary due diligence. Identification documentation may or may not be passed on.

98. In considering the role of third parties in the identification process, the starting point must be the general rule that the entities subject to these obligations must identify all customers (including beneficial owners or controllers) and verify the documents or information. Any exceptions to this rule should be strictly limited. However, the FATF accepts that provided that there are appropriate safeguards and controls, reliance on a third party to perform certain elements of the due diligence procedures is acceptable within the FATF framework, and this section considers what could be appropriate.

99. The section also considers the extent to which the FATF should seek to lay down standards or guidance on what is acceptable, and whether certain issues or questions of detail should be left to individual countries to determine. Any amendments to the Recommendations or guidance on this issue will be of a permissive nature, i.e. it would permit countries to authorise their institutions to rely on a third party in particular circumstances, but would not require them to do so.

3.5.1. Measures currently in place

100. At a national level, some FATF members allow the institutions that are subject to customer identification and verification obligations to rely on third parties to perform some of those processes. The different positions that are taken by FATF members that allow this reliance on third parties are set out in Annex 3. What is important to note though, is that the responsibility for identification and verification continues to rest with the primary institution. In an operational sense, the primary institution responsible can rely on a third party, but this does not transfer the responsibility of the primary institution to the third party.

101. In relation to international standards or guidance, the Basel CDD paper considers the issue at section 2.2.3 (Introduced business), and accepts that it is reasonable to rely on a third party, although the responsibility always rests with the recipient bank. The Basel CDD paper (which only sets standards or guidance for banks) lays down various principles and criteria, which a bank should consider when deciding whether to rely upon a particular introducer:

- "it must comply with the minimum customer due diligence practices identified in this paper;
- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- the bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the financial intelligence unit or equivalent enforcement agency, where appropriate legal authority has been obtained.

In addition, banks should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above."

102. The International Association of Insurance Supervisors (IAIS) also issued guidance on this issue in January 2002. In section 9.5.1 the Guidance Notes lay out the circumstances in

which an insurance entity[15] can rely upon an introducer to verify the identity of the client they are introducing. A basic precondition for any reliance upon the introducer is that the introducer will complete verification of all such customers, will keep records in accordance with the Guidance Notes, and will supply copies of those records upon demand. The insurance entity can then rely upon the third party introducer to verify identity if:

- It is a reliable local introduction, preferably in writing.
- The introducer is:
  (i) a professionally qualified person or independent financial adviser operating from an acceptable jurisdiction, and
  (ii) the insurer is satisfied that the rules of his/her professional body or regulator include ethical guidelines, which taken in conjunction with the money laundering regulations in that jurisdiction include requirements at least equivalent to the Guidance Notes, and
  (iii) is reliable and in good standing and the introduction is in writing, including an assurance that evidence of identity will have been taken and recorded.
- Verification is not needed where the introducer of a prospective policyholder is an overseas branch or member of the same group as the insurance entity.

103. There are several types of insurance intermediaries (agents and brokers): (a) a broker (in theory independent of any company), (b) an agent that is employed by the company, (c) an agent of the company that is self-employed, and (d) other institutions that refer business e.g. banks. IAIS estimate that a large percentage of individual life policies come through intermediaries, and the position of the IAIS set out in the Guidance Notes is that it is essential that both the insurance companies and the insurance intermediaries must be subject to anti-money laundering obligations.

104. Although the EU Directive does not expressly refer to situations in which reliance could be placed on third parties to perform identification functions, article 3(10) allows EU member states to deem identification requirements to be met where payment of an insurance premium is made from an account at an EU bank in the name of that customer. In effect this results in the insurance company relying on a third party bank to verify its customers, and is based on the assumption that the bank from which the payment is made will have properly performed the necessary identification and due diligence, and that there is no need to re-verify the person's identity.

3.5.2. Outsourcing and agency arrangements

105. The normal customer identification and verification obligations are predicated on the basis that these functions are carried out by officers or employees of the financial institution. However, having regard to the diversity of the financial sector, there may be many occasions when these functions are performed by agents or are otherwise outsourced. This is an important issue, because the percentage of financial functions which is being outsourced is increasing, and there is a need to determine whether the agent or other person acting for the financial institution is subject to the same or similar anti-money laundering and due diligence obligations that apply to the institution. If so, and the institution receives all the records then

[15] Under the Guidance Notes, the insurance entity also includes agents or brokers that introduce business.

there is effectively no reliance on third party identification (the agent could be treated similarly to an employee). If not, then one needs to consider the rules that apply to introduced business. These are likely to include requirements that the third party is subject to appropriate due diligence requirements. In the insurance sector, one approach that has been taken in relation to agents and brokers, where they are not subject to legislative due diligence obligations, has been for insurance companies to impose contractual due diligence obligations on the agent/broker. In any event, this needs further examination in the context of common business practices in each of the major financial sectors.

3.5.3. Reliance on third parties (other than outsourcing and agency arrangements)

106. The central issue is to define the circumstances in which an institution or entity that is subject to customer due diligence obligations may rely on a third party to perform some or all of the identification and verification processes[16]. A number of factors are relevant to an overall policy:

a) The types of institutions or entities that can "delegate" certain elements of the processes, and any obligations they might have if they do this.
b) The identification elements that can be performed by third parties.
c) The classes of third parties that may be relied upon, and the preconditions for eligibility.
d) The jurisdictions from which the third parties could come.

107. Whatever system is adopted, a key principle under any system that relies on third party identification or verification of identity is that the institution or entity that is relying on the third party always has the ultimate responsibility to know its customers, even if it transfers certain elements of the procedures.

108. In considering this issue, the FATF has prepared a draft statement setting out the conditions pursuant to which a financial institution or other entities could rely on a third party to perform the identification and/or verification functions. The draft proposal contains a set of general principles, followed by various options offering alternative approaches for implementing those principles. There are also a number of other issues set out, on which the FATF seeks comments.

Reliance on third parties to perform certain elements of the due diligence process concerning identifying customers and verifying identity

FATF's initial view is that:

Certain entities can rely on third parties to perform certain elements of the procedures for identifying customers (including the beneficial owner) and verifying their identity in order to be placed in a position to decide whether the identification conditions to enter into a relationship with a customer are fulfilled.

[16] These are set out at paragraph 30 above – (a) identify the customer, (b) verify the identity of the customer, (c) identify the beneficial owner, (d) verify the identity of the beneficial owner. Other elements of a customer due diligence policy such as accepting the customer, on-going assessment and risk management are matters that could not normally be handled by a third party.

The ultimate responsibility for the overall identification and verification procedure remains with the entity that enters into the customer relationship.

The entity relying on the third party must satisfy itself as to the adequacy of the identification information it receives.

All relevant data and documentation pertaining to the customer's identity should, in relation to banks, be immediately submitted, and, in relation to other entities, be immediately submitted [or immediately made available on request] by the third party to the entity that enters into the customer relationship. Such information must be available for review by the supervisor, or law enforcement agencies or the FIU, where appropriate legal authority exists.

The entity relying on the third party should always be able to request additional information about the customer.

An entity is permitted to rely on third parties if the entity:
- is subject to the full range of AML requirements set out by FATF for that type of entity;
- is subject to a certain minimum level of supervision and regulation;
- satisfies itself, on a regular basis, about the reliability of the systems used by the third party to identify and verify customer identity.

A third party must:
- have customer identification and verification practices that are as rigorous as those that the entity that enters into the relationship would have conducted itself for the customer;
- enter into a written agreement with the entity that enters into the relationship with the customer in order to determine how the identification and verification procedures will be performed.

Issues, still requiring further consideration by the FATF, include:

1. What types of "entities" could be permitted to rely on third parties

Option 1
Financial institutions as defined in section 3.1 that are subject to the regulation and supervision standards in section 3.8 of this paper

Option 2
All entities in a jurisdiction that are subject to the full range of AML requirements including the regulation and supervision standards in section 3.8 of this paper.

2. Who can be a third party

Option 1
Financial institutions as defined in section 3.1.

Option 2
All third parties in a jurisdiction that are subject to the full range of AML requirements including the regulation and supervision standards in section 3.8 of this paper.

Option 3
Any third party that the entity is satisfied meets the first four bullet points of the Basle CDD standards for introduced business[17] and which is a member of a class of persons or entities that the jurisdiction determines are acceptable to be third parties (See Basel CDD paper at paragraph 36).

3 What level of supervision and regulation is required for the third parties

Option 1
They must be subject to the regulatory measures set out in section 3.8. below.

Option 2
In addition to option 1, they must be subject to the supervision of a public authority empowered with administrative or criminal sanctions.

Option 3
Third parties which are not subject to any public authority supervision but which are capable of complying with and do comply with the CDD criteria. They would need to be subject to periodic reviews by the entity that is relying on it consistent with the principles in the Basel CDD paper.

109. There are also a number of ancillary issues, where the FATF also seeks the views of interested parties. These concern:

a) Document retention - Once the customer identification and verification obligations have been performed by the third party and the process properly documented:

   (i) Should the customer identification information be immediately submitted or is it acceptable if it is immediately made available on request?
   (ii) If the information is to be submitted, must it be obtained before a business relationship is established or is it acceptable for the information at a later date, and if so, by when (see also section 3.6.2. below).

b) Is a different set of requirements for non-banks acceptable given the requirements imposed on banks by the CDD paper?

c) NBFI - Are there any particular implications that arise from the applying these concepts to non-bank financial sectors.

d) Chains - Should "chains" of third parties be allowed, and if so, in what circumstances or subject to what conditions?

[17] The issue of the criterion in the CDD paper relating to when information must be submitted is a separate consideration outlined above. For banks the third party must meet all of the requirements in the CDD paper, including bullet point 5.

3.5.3.1 Third parties from which jurisdictions

110. In which countries and jurisdictions could the third parties that meet the conditions be based? It seems appropriate that it should apply to countries and jurisdictions that have anti-money laundering and due diligence requirements, which are equivalent to the FATF framework (as revised). This would provide a sound basis for action, but the difficulty would be how to assess and apply this in a fair, objective and meaningful way. As can be seen from Annex 3, FATF members that allow third parties to perform identification and verification functions allow it to be done in relation to a variety of jurisdictions. It is also a significant issue for the financial sector, since customer identification and verification rules can have significant cost implications, and the financial sector continually seeks information on which jurisdictions have anti-money laundering measures that meet FATF standards.

111. There appears to be several possible ways to address the question of whether there are equivalent standards in place. In deciding which approach is feasible, there should be an objective analysis of the measures in place:

- **Option 1** - Leave it to each jurisdiction to determine. The FATF could set out the preconditions under which an institution or entity could rely on a third party e.g. as set out above. Each jurisdiction would then be responsible for assessing whether other countries and jurisdictions meet or do not meet the FATF standards. Leaving it to each jurisdiction is the current position, which has the advantage that it reduces the difficult work that the FATF would have to do on this issue, but the disadvantage that the playing field is likely to be uneven. For example, global financial institutions could find that their branch in jurisdiction A can rely on a third party in jurisdiction B, but their branch in jurisdiction C cannot do so – a situation that is somewhat anomalous. When assessing the judgements made by each jurisdiction FATF could take into account whether that jurisdiction had made its decision consistent with known mutual evaluation reports, any NCCT lists published by FATF, other assessments published by other agencies (e.g. IMF FSAP or OFC assessments, etc).

- **Option 2** – Leave it to each institution to decide whether the standards applicable to and applied by the third party are sufficient, in accordance with the principles laid down in the Basel CDD paper – the institution would continue to bear ultimate responsibility even where it relied on third parties to perform certain functions. Although consistent with the approach of the Basel CDD paper, this may lead to diverse results, even within a jurisdiction.

112. The FATF also considered the options for issuing either a positive minimum list of jurisdictions that meet the necessary FATF anti-money laundering standards, or a negative list of jurisdictions that fail to meet those standards. However, it was decided that the FATF would not be in a position to assess the anti-money laundering systems in all jurisdictions with a view to assessing whether it would be reasonable to rely on a third party performing identification or verification functions in those jurisdictions, and that therefore neither of these options would be feasible.

3.5.4. Recommendation or Guidance

113. It is probably not feasible or realistic to consider putting all the detailed issues raised in this section of the paper, or even the proposed solution set out above, into the Recommendations. The issues and the solution could be recognised in the Recommendations, preferably in a single sentence or set of bullet points that cross references to guidelines that will spell out in more detail the issues, the minimum requirements and the best practice. Such guidelines would also include other issues of detail.

114. The issues that are discussed in this section of the paper are detailed ones, but they are important in that there are significant implications for the institutions that are subject to obligations to identify their customers. It is also important that the Recommendations or subsidiary guidance address issues, which might otherwise be thought to be inconsistent with the Recommendations. This paper therefore seeks to highlight the various approaches that are taken, whether by FATF members or by other international organisations, such as the Basel Committee, and then suggests possible solutions for addressing these issues.

3.6. Other specific issues requiring clarification

3.6.1. Requiring financial institutions to identify all customers, including existing customers

115. Currently, Recommendation 10 requires financial institutions to "identify their clients … when establishing business relationships or conducting transactions". This has been consistently interpreted, both within FATF and elsewhere as an obligation to identify clients when they open an account or otherwise establish a new relationship i.e. in the future and only after these events occur. Customers that held accounts established prior to the time that various national legislative identification requirements came into effect (mostly between 1990-95), and who did not open new accounts or did not conduct large cash or suspicious transactions, may not have had their identity verified.

116. Different approaches have been or are being taken within jurisdictions, with some jurisdictions only requiring new customers to be identified, while others require all customers, including existing ones, to be identified. It is reasonably clear that the Forty Recommendations do not currently require the identity of customers that held accounts prior to the introduction of the relevant national identification obligation to be verified. However, the issue was highlighted in the FATF NCCT exercise, and was deferred for further consideration under the review of the Recommendations. In the June 2000 NCCT report, the issue was stated as:

> "(v) The lack of a stringent scheme to apply the new rules of customer identification for accounts open prior to their entry into force."

117. The lack of customer identification requirements for pre-existing accounts does create an increased risk with respect to money laundering, and does create the potential for old accounts to be misused, though it is not clear how materially significant that risk is. A requirement to identify all customers would help minimise that risk, but against this must be weighed the additional costs. It has been suggested that a universal requirement to identify all customers would be very onerous in large jurisdictions with many institutions, customers and accounts. Despite this, legislation requiring the identification of existing account holders has been implemented in both large and small jurisdictions. Another argument made against such a requirement is that verified identification will gradually take place over time anyway, under existing anti-money laundering laws and regulations, and that in the meantime, a degree of protection is provided by the obligation to report suspicious transactions.

118. The Basel CDD paper suggests that customer identification and verification could be applied to existing account holders but on the basis of materiality and risk assessment. However it also recognises that the FATF is currently considering the issue. The relevant text from the Basel CDD paper states:

> "24. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records*. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks

sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

* The application of new KYC standards to existing accounts is currently subject to FATF review."

119. The options that the FATF could consider comprise:

Option 1
Confirming that the approach in the Basel CDD paper is appropriate [for financial institutions and reflect that approach in the FATF framework.

Option 2
Amending the FATF 40 to explicitly require that financial institutions are required to verify the identity and conduct due diligence for all their customers, including existing customers, and either:
- Require that this be done in a reasonable time frame; or
- Set a fixed period e.g. 5 years after the relevant requirement comes into force in which that must be done.

3.6.2. Timing of verification of identity

120. When accepting new customers, at what point in time should the new customer's identity be verified i.e. before the account is opened, after the first payment into the account but before any withdrawal is made or securities are purchased etc? Some jurisdictions provide that accounts should not be opened unless verification has taken place, others allow initial deposits to be made without verification but not withdrawals or other transactions, while in other jurisdictions institutions are allowed to open an account and do the verification as soon as possible afterwards. Timing of verification is a matter that is also important for "non-face-to-face" customers.

121. This issue was considered in the Basel CDD paper, which states:

"22. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified."

122. The options that the FATF could consider, comprise:

Option 1 - Amend the FATF Recommendations to explicitly require financial institutions to verify their customer's identify before [a relationship is established (*as per the Basel CDD paper*)] [the customer is able to withdraw any funds or conduct securities transactions from the account]. Additional guidance may also need to be formulated to clarify the point at which a relationship is established for different types of business.

Option 2 - Amend the FATF Recommendations to explicitly acknowledge that financial institutions can open accounts without having verified the customer's identity so long as they do so as soon as reasonably practicable afterwards.

Option 3 - Issue best practice guidelines (with an expectation that verification would usually take place before accounts are opened but recognising that there will be some circumstances where this will not be practical and outlining the factors that might indicate whether or not the customer should be able to withdraw funds before verification takes place).

3.6.3. Identification when money laundering suspected or for occasional customers

123. Recommendation 10 currently requires that the identity of occasional customers be verified and recorded if they conduct large cash transactions. There is no express identification or verification requirements for financial institutions if an institution suspects that a transaction relates to money laundering, though in some jurisdictions this obligation may be an implied part of the reporting obligation. Under article 3(2)&(8) of the recently amended EU Directive, and pursuant to legislation in almost all FATF members, financial institutions are required to identify their clients if they suspect that a transaction relates to money laundering, or if an occasional customer conducts either one, or several related transactions, which exceed the threshold for identification. The EU Directive sets the minimum threshold for identification transactions conducted by occasional customers at € 15,000. The threshold for identification of occasional customers conducting transactions in FATF members is as follows:

Transaction threshold for identification of occasional customers	
Threshold (USD/€)[18]	Member
2,000	Canada
2,500	Hong Kong, China[19],
4,000	Turkey[20]
5,000	Brazil, New Zealand
7,000	Australia
8,000	France
10,000	Argentina, Belgium, Italy, Luxembourg, Mexico, United States, the Kingdom of the Netherlands
12,000	Ireland, Norway, Portugal, Singapore
13,000	Sweden
15,000	Austria, Denmark, Finland, Germany[21], Greece, Iceland, Spain, Switzerland, United Kingdom
300,000	Japan[22]

[18] Calculated to nearest USD 1,000, and based on exchange rates of approximately $1 = €1

[19] Obligation imposed on money remittance agents and bureaux de change (by law), and banks (by guidance), to identify all occasional customers that have remittance or exchange transactions above HKD 20,000, and record the required details.

[20] The amount is 2 billion Turkish Lira, indexed to the exchange rate.

[21] A lower threshold of USD 2,500 is recommended for currency exchange and money remittance.

[22] The threshold is currently under consideration.

124. There is general support for the inclusion of an explicit obligation to identify the customer when it is suspected that a transaction relates to money laundering, or if there is a single or several related transactions by an occasional customer, which together exceed the threshold for identification. Concerns have also been expressed where thresholds for identification for large transactions are very high and it is suggested that the FATF should consider how to introduce greater consistency on this issue. As can be seen above, almost all FATF members require identity to be verified when there is a single or several linked transactions above USD/€ 15,000, though some members have a lower threshold.

125. Although there are very different national and cultural practices concerning the use of large amounts of cash, FATF members have recognised the desirability of using other payment and transfer methods. Recommendation 24 expressly encourages the replacement of cash transfers by other techniques of money management. Given this objective, the benefits of greater consistency and certainty, and having regard to the table above, it is proposed that the FATF set a minimum threshold for large transactions by occasional customers, above which verification of identity would be required. This would be the case whether the transaction is carried out in a single operation or in several operations, which seem to be linked. Options that the FATF could consider concerning the threshold include:

Option 1
Agreeing a minimum threshold amount, for example USD/€ 15,000, and setting this out as part of sound practice guidance.

Option 2
Including the minimum threshold in the Recommendations (members could set a stricter threshold if they so desire).

126. It is accepted that if there is a suspicion of money laundering then the customer, whether permanent or occasional, should be identified. This should apply irrespective of any exemption that might otherwise apply, or any transaction threshold that is laid down above. It is proposed that the FATF Recommendations be amended to require customer identification in these circumstances, i.e. whenever there is a suspicion of money laundering. FATF is interested in receiving comments about this proposal, and in particular, how the obligations might interact with practical issues such as the risk of tipping off, or where suspicion arises after the transaction has been completed.

3.7. Suspicious Transaction Reporting

127. A number of issues concerning suspicious transaction reporting[23] that may require amendments to the FATF 40, and which are not dealt with elsewhere, have been identified.

3.7.1. The Financial Intelligence Unit (FIU)

128. It is widely accepted that a financial intelligence unit (FIU) is a necessary part of a suspicious transaction reporting system, and that the Recommendations should explicitly refer to the need for such a body. Article 7(1)(b) of the United Nations Convention against Transnational Organized Crime (the Palermo Convention) expressly refers to the need for an FIU:

> "1. Each State Party:
> ……
> (b) Shall, without prejudice to articles 18 and 27 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering."

129. This description of an FIU contained in the Palermo Convention appears to be closely based on the Egmont Group definition of an FIU:

> "A central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information
>
> (i) concerning suspected proceeds of crime, or
> (ii) required by national legislation or regulation,
>
> in order to counter money laundering."

130. As in other parts of this paper, the FATF has found it desirable to rely on existing international standards, and to cross-reference those standards within the FATF 40 where appropriate. The concept of an FIU has already been defined by the Egmont Group, and it seems undesirable to repeat that definition. The FATF therefore intends adding wording that requires countries to establish an FIU:

> "Countries should establish an FIU, as defined by the Egmont Group of financial intelligence units, to serve as a national centre for the collection, analysis and dissemination of suspicious transaction reports and other information regarding potential money-laundering."

[23] The Netherlands has a system based on the reporting of unusual transactions (rather than suspicious transactions).

3.7.2. Feedback for suspicious transaction reporting

131. It is widely accepted by governments and financial institutions that it is necessary for feedback to be provided to reporting institutions, whether specific feedback on individual STRs or feedback of a general nature. The 1998 FATF Best Practice Guidelines[24] on the issue already set out detailed guidance on the different types of feedback that can be provided, and the objective is how to ensure that feedback is part of the STR systems in all countries. It is proposed that a short reference to the need for feedback and to the Guidelines be included in the Recommendations, and two alternate sets of wording are suggested for current Recommendation 18:

Option 1

"18. Financial institutions reporting their suspicions should comply with instructions from the FIU and other competent authorities where applicable. The FIU should provide feedback on suspicious transaction reports in accordance with the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons."

Option 2

"18. Financial institutions reporting their suspicions should comply with instructions from the FIU and other competent authorities where applicable. In order to enhance suspicious transaction reporting in each jurisdiction, FATF encourages the FIU in each jurisdiction to provide feedback on suspicious transaction reports in accordance with the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons."

3.7.3. The scope and nature of the reporting obligation

3.7.3.1. Indirect reporting

132. This is an issue that was highlighted in the NCCT exercise, and which was deferred for further consideration under the review of the Recommendations. In the June 2000 NCCT report, the issue was stated as:

> "The practice in some jurisdictions of an "indirect obligation" to report suspicious transactions related to some criminal offences, whereby making a report provides a defence against a charge of money laundering, rather than a direct obligation to make a report."

133. In some countries this "indirect obligation" is supported by regulatory requirements on financial institutions to implement internal reporting procedures designed to lead to suspicious transaction reports being made. This can be compared with the obligation in Recommendation 15, which provides:

[24] See http://www.fatf-gafi.org/pdf/FEEDB_en.pdf

"15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities."

134. The 25 NCCT Criteria also impose an obligation to have an efficient mandatory system for reporting suspicious or unusual transactions:

"(v) Lack of efficient suspicious transactions reporting system

10. Absence of an efficient mandatory system for reporting suspicious or unusual transactions to a competent authority, provided that such a system aims to detect and prosecute money laundering.

11. Lack of monitoring and criminal or administrative sanctions in respect to the obligation to report suspicious or unusual transactions."

135. It has been said that the indirect obligation to report is the equivalent of a direct, mandatory system. One argument is that STR are made by reporting institutions because the transaction is out of the ordinary, the institution does not usually know the underlying crime, and therefore it reports because of the indirect obligation imposed through the money laundering offence. Another argument is that the potential consequences of not reporting under "direct" or "indirect" systems are the same i.e. that a person with the relevant suspicion could be liable to prosecution.

136. Counter-arguments include:

- In most jurisdictions the elements of a money laundering offence will be much more difficult to prove than an offence of failing to report. This would mean that the indirect obligation may not have the same consequence as a direct obligation.

- As the indirect obligation is less precisely determined, it will be more difficult for competent authorities to exercise effective control over, and impose sanctions on the reporting institutions, where necessary. The indirect obligation also only allows for a criminal sanction to be imposed as opposed to administrative sanctions, which may provide a satisfactory alternative in some circumstances.

137. The options that the FATF could consider, comprise:

Option 1 - Leave it to each country to decide how to implement their reporting requirements.
Option 2 - Amend the FATF framework to recognise that "indirect reporting" is acceptable.
Option 3 - Amend the FATF framework to require that there be an explicit obligation by law or regulation to report suspicious transactions, to take into account NCCT Criteria 10 & 11, and to provide appropriate sanctions for failure to comply.

3.7.3.2. Reporting on the basis of suspicion or reasonable grounds to suspect

138. Recommendation 15 requires financial institutions to file reports with the competent authorities when they "suspect" that funds stem from a criminal activity. Recommendation

IV of the FATF Special Recommendations on Terrorist Financing requires reports to be filed when institutions "suspect or have reasonable grounds to suspect." Almost all FATF members (as well as many other countries) have a reporting requirement based on either “suspects" (subjective), or "reasonably suspects" or "has reasonable grounds to suspect" (objective). A few countries have a test that uses a higher level of mental certainty such as "strong suspicion" or "well-founded suspicion". One member has a system based on the reporting of unusual transactions.

139. A requirement to report when the individual "suspects" is a subjective test of suspicion and requires proof to be supplied that the individual actually suspected that a transaction involved a criminal activity. A requirement to report when there are "reasonable grounds to suspect" is an objective test of suspicion and can be satisfied if the circumstances surrounding the transaction would lead a reasonable person to suspect that the transaction involved criminal activity. With the objective test it is not necessary to prove that the individual actually suspected illegality, just that a reasonable person should and would have suspected. The objective test is generally regarded as a slightly wider reporting requirement than a subjective test. It would, for example, catch someone who did not report because of a negligent failure to recognise suspicion even if as a result of this negligence, they really did not suspect that the transaction had a criminal source.

140. The first issue for consideration is whether Recommendation 15 should be amended to make it consistent with Recommendation IV, and with the measures that have been taken at a national level. There are two alternative ways to address the issue:

Option 1 - to amend Recommendation 15 by changing the words to "suspect or have reasonable grounds to suspect", instead of just “suspect”. These words require countries to have either one of the two alternatives, but not both.
Option 2 - to amend both Recommendation 15 and Recommendation IV and change the words in both Recommendations to "have reasonable grounds to suspect"

3.7.3.3. Attempted transactions

141. An issue which was identified in the mutual evaluations of several FATF members was the lack of an obligation to report when a financial institution chose not to enter into a transaction which they suspected was linked with money laundering. While financial institutions are not prevented from terminating a relationship with a suspicious client, or refusing to enter into a transaction, it is clearly desirable that attempts to launder money be reported. The consequence of not doing so is that a criminal would then be able to approach other institutions until one was found that did not find the transaction suspicious. It would be desirable in many cases that institutions report the suspicious transaction and then proceed in accordance with instructions from the FIU (in line with Recommendation 18). However, the requirement to report attempted transactions is not explicitly stated in Recommendation 15. There are two alternative ways to address the issue:

Option 1 – to amend the Recommendation to expressly include reference to attempted transactions.
Option 2 – amend the Interpretative Note to Recommendation 15 to clarify that attempted transactions should also be reported.

3.7.3.4. Suspicious activity

142. Recommendation 15 currently refers to suspicious transactions (although the Recommendation refers to "funds", FATF processes and anti-money laundering systems commonly refer to "suspicious transaction reporting"). In some countries there is a wider obligation to report, which applies to suspicious activity. This would not only include circumstances where there is a financial transaction, but could also cover the giving of financial or other advice. This issue is particularly important when considering the application of a reporting obligation to some of the categories of non-financial businesses or professions covered in section 5 of this paper, such as trust and company service providers, lawyers or accountants. The services offered by these businesses or professions may not involve them conducting a financial transaction for their customers, but, as noted in that section, professional advice or the creation of a chain of companies or trusts is often essential to more complex money laundering schemes.

143. A different approach is also taken in the EU Directive, which does not refer to funds or transactions. Article 6(1) of the Directive states:

> "Institutions and persons subject to this Directive and their directors and employees cooperate fully with the authorities responsible for combating money laundering: (a) by informing those authorities, on their own initiative, of any fact which might be an indication of money laundering …"

144. The FATF recognises that there would need to be a level playing field, and that an obligation to report suspicious activity could not apply just to certain classes of non-financial businesses or professions, but if adopted, would need to apply to all reporting institutions or entities. It is also important that any revised obligation should address the money laundering risks and threats and should not impose overly broad requirements. The FATF seeks comments on the possible extension of Recommendation 15. Options include:

Option 1 – to amend Recommendation 15 to cover suspicious activity that is linked to the proceeds of a criminal activity.
Option 2 – to amend Recommendation 15 in a limited way, to cover particular types of business transactions or advice that have a higher risk of being misused for money laundering.
Option 3- Leave it to each country to decide how to implement their reporting requirements.

3.7.3.5. The criminal activity that should be reported

145. The FATF is considering clarifying the requirement in Recommendation 15 to file reports when it is suspected that funds stem from "a criminal activity". This would also take into account the 25 NCCT Criteria, where criterion 10 states "*absence of an efficient mandatory system for reporting suspicious or unusual transactions to a competent authority, **provided that** such a system aims to detect and prosecute money laundering.*" (Emphasis added).

146. A large majority of FATF members have legislation that requires reporting when funds or assets are suspected to be related to a money laundering offence (including the applicable predicate offences). In some members the obligation to file reports of suspicious transactions relates to a wider range of offences than the predicate crimes for the money laundering offence. In some other members the offences underlying the reporting obligation are narrower than the predicate crimes for the money laundering offence. At a practical level, financial institutions have indicated that they usually cannot determine the precise illegal source of the suspicious funds.

147. The alternative approaches that the FATF is considering to address this issue are:

Option 1
Provide additional clarification in the Recommendations to indicate that STR should be made for all crimes.

Option 2
Provide additional clarification in the Recommendations to indicate that for each country the offences underlying the obligation to report should not be narrower than the scope of the predicate offences underlying the money laundering offence.

Option 3
Leave it to each country to decide how to implement their reporting requirements.

3.8. Financial Sector Regulation and Supervision

148. This section of the paper deals with the issue of the regulatory standards that are required in relation to the financial activities covered under the FATF framework.

3.8.2. ***The existing FATF framework***

149. Summaries of those portions of the current FATF 40, the NCCT Criteria and the Special Recommendations on Terrorist Financing that apply to regulation and supervision issues are set out below. The full text of the relevant material is attached at Annex 4 with the pertinent parts highlighted in bold.

150. The current FATF 40:

- Recognise that not all NBFIs will be subject to a formal prudential supervisory regime - but requires the AML measures to be applied to NBFIs and that the laws are implemented effectively (R 8).
- States that, as a minimum requirement, FATF members should have an effective system whereby bureaux de change are known or declared to the relevant authorities and that the AML measures be applied to bureaux de change (Interpretative note to R 9).
- Require competent authorities to ensure that the supervised financial institutions have adequate programs to guard against money laundering (R 26). There is no statement about precisely which institutions should be supervised or how the competent authorities should discharge their obligation.
- Requires competent authorities to be designated to carry out administrative supervision and regulation, in other professions dealing with cash to ensure an effective implementation of the FATF 40 (R 27).
- Expects legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates' (R 29). However, the framework does not expect a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but stresses the desirability of conducting "fit and proper" checks on controlling shareholders (Interpretative Note to R 29).

151. The NCCT Criteria indicate that:

- Jurisdictions should have effective regulation and supervision for all financial institutions with respect to "international standards applicable to money laundering". (NCCT 1)
- Individuals or legal entities should not be able to operate a financial institution without authorisation or registration or with very rudimentary requirements for authorisation or registration. (NCCT 2)
- Measures are needed to guard against holding of management functions and control or acquisition of a significant investment in financial institutions by criminals or their confederates. (NCCT 3)

152. The Terrorist Financing Recommendations require that:

- Alternative remittance providers should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions (TF SR VI).
- Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions (TF SR VI).

3.8.2. ***Regulatory approach***

153. The key regulatory objectives that might be drawn from the words already in the FATF framework seem to be that all financial institutions are:

- Subject to legal or regulatory measures to guard against control or acquisition of them by criminal elements.
- Subject to the AML measures.
- Complying with AML measures
- Able to be prosecuted or otherwise sanctioned for non-compliance with AML measures.

154. The FATF framework does not have detailed requirements concerning the type of regulatory or supervisory regime it expects to achieve these objectives. Nevertheless, minimum standards are expressed for some types of entities (e.g. money remitters must be licensed or registered, bureaux de change must be known to the authorities). The broad obligation is that jurisdictions must ensure that the FATF framework is complied with.

155. Moreover, the FATF framework currently suggests that it is not meant to impose a prudential financial sector regulatory regime unless that is consistent with other public policy objectives. For example regulation of bureaux de change may be less intense in jurisdictions with a liberal foreign exchange control regime than in jurisdictions that have strong foreign exchange controls/restrictions. The obligation is to impose appropriate regulation and supervision regarding AML measures.

156. Jurisdictions impose regulation in the financial sector for a variety of reasons. These include:

- To provide assurances to and protection for customers and investors.
- For prudential/systemic protection.
- Because the jurisdiction believes this is necessary for effective AML regulation.
- To facilitate competition.
- To generate revenue/impose quota limits on the number of financial service providers operating in a sector.
- To ensure controlled not market driven growth.
- For other social and economic objectives.

157. The response to market failures and the underlying macroeconomic framework is not the same in all jurisdictions. Moreover, the costs versus benefits of various solutions are different for each jurisdiction. Accordingly, this suggests the need for flexibility in FATF's approach to what is required in the area of financial sector regulation and supervision for the purposes of anti-money laundering.

158. Nevertheless, the underlying objectives of the FATF framework are broadly consistent with most of the reasons that jurisdictions already regulate their financial sector. Moreover, the overall objective of the FATF framework (minimising the ability of criminals and terrorists to use the financial system for their illicit purposes) is consistent with the risk management objectives of financial institutions. Accordingly, the application of the FATF 40 to most financial institutions in a jurisdiction should not require the imposition of many requirements to those that might already exist.

159. The approach of many FATF jurisdictions is to "add on" their AML measures to existing financial sector regulation and supervision. However, with a trend towards the proliferation of financial institutions as technology breaks down traditional business models, it may not be appropriate to focus on this approach, especially if the objectives of the financial sector regulators are not concerned with AML measures as is the case in some jurisdictions. Accordingly, while some international prudential standards might be appropriate, the core underlying issue for FATF is that the core AML measures are applied to it/them and that the financial institutions are complying.

160. A spectrum of different types of financial sector regulation/supervision might be described, in increasing order of intensity:

- No licensing, registration or supervision at all.
- Rules or laws permitting or restricting activities being in place.
- Prohibitions on criminals from being able to manage or control financial service providers in place.
- Persons carrying out the activity are known to competent authorities.
- Generic corporate/entity registration (i.e. corporations law in place).
- Functional or entity registration (name of entity added to list and then entity is allowed to carry out activities, no discretion to reject application).
- Functional or entity licensing (competent authority evaluation of entity against criteria and then entity is allowed to carry out activities. Criteria may or may not include a “fit and proper person” assessment.).
- Self-regulatory oversight of certain types of entities (e.g. lawyers).
- Functional or entity monitoring (oversight/observation by competent authorities).
- Functional or entity supervision (evaluative assessment of ongoing operations). The extent varies:
  - Administrative guidance versus rules and prohibitions.
  - Reliance on internal/external auditors for assurances.
  - Off site versus on-site checking.

161. Moreover, there might be a positive-list or negative-list approach to licensing/registration/regulation i.e. licensed or registered entities are allowed to carry out a list of activities or licensed or registered entities are able to carry out any financial activity unless that activity is specifically prohibited.

162. In addition, the quality of implementing the regulatory framework could vary, meaning that a jurisdiction that “on paper” appeared to have a “strong” regulatory framework could in practice have a weaker regime of compliance with AML measures than a jurisdiction that had adopted a less intensive regulatory approach that was implemented more effectively. Moreover, there is mixed evidence about which level of intensity of supervision results in the best legislative compliance.

163. The method for gaining assurance that different types of entities are complying with the core AML measures could vary according to contextual factors such as:

- The known or suspected levels of criminal activity in that jurisdiction and/or financial service providers of that type.
- The known or suspected levels of money laundering/terrorist financing activity in that jurisdiction and/or financial service providers of that type.
- The known or suspected levels of corruption in that jurisdiction and/or financial service providers of that type.
- The size of that sector or activity in the jurisdiction.
- Other regulatory matters that encourage high standards of financial sector or corporate sector behaviour in the jurisdiction.
- The incentives for legislative compliance (levels of criminal or civil penalties for non-compliance) and the culture of legal compliance in that jurisdiction.

164. The higher the level of risk of money laundering/terrorist financing or lack of compliance in a jurisdiction or industry sector within a jurisdiction, the more intensive the level of regulation and the method for gaining assurance needs to be.

165. Evidence of the level of risk in a jurisdiction or industry sector might be drawn from:

- Crime levels.
- The number of cases commenced and conviction levels for money laundering or terrorist financing.
- Typologies reports indicating the level of money laundering/terrorist financing activity.
- "Failed" investigations that uncover poor compliance with AML measures.
- Evidence that the jurisdiction or financial institutions within the jurisdiction are being used by criminals or for financing terrorism.
- The experience and evidence of other jurisdictions in relation to above matters concerning the jurisdiction being reviewed or evaluated.

166. The minimum level of regulation for entities seems to be that they are subject to a regulatory framework that achieve the core AML measures objectives mentioned above irrespective of the licensing, registration or supervision regime that applies to them.

167. While it seems reasonable that there might also be a need to know whether financial institutions exist or not or that they are licensed or registered there is probably less consensus as to whether this should be mandatory for all types of institutions or financial activities - although this is a position that FATF could adopt. It is clearly the expectation for banks and other major types of institutions. FATF has also determined that bureaux de change should be known to authorities and that money remitters should be licensed or registered because of the particular money laundering/terrorist financing threats that they present in many jurisdictions. However, many minor or fringe financial institutions, including some money service businesses, are not currently subject to registration or licensing regimes in some jurisdictions. Some view this as a weakness in international efforts to combat money laundering and terrorist financing. Others see it as acceptable given other institutional or contextual factors that exist to minimise the money laundering risk.

168. The minimum level of monitoring or supervision for financial institutions where there is no applicable international supervisory standard seems to be that the competent authorities/FIU must monitor compliance with the core AML measures through actively analysing and investigating:

- A lack of suspicious transaction reports from sectors or financial service providers within sectors.
- Poor quality suspicious transaction reports.
- Any evidence from criminal investigations that financial service providers should have filed suspicious transaction reports and did not.
- Any evidence from criminal investigations that financial service providers did not follow the required AML measures (e.g. did not carry out customer identification or did not keep financial records).

Investigating seems to at least to require powers to:

- conduct on-site inspection or gain assurance from the likes of an auditor about compliance; and
- impose civil or criminal sanctions where non-compliance is uncovered.

169. Above these minimum levels the FATF framework seem to imply an expectation that jurisdictions will apply an appropriate level of regulation and supervision for each type of entity/financial activity according to the risks – with an underlying assumption that the prudential regulation and supervision regime automatically extends to AML measures. Moreover, for some institutions/activities there will also be international supervisory standards issued by other organisations. The NCCT exercise concluded that in addition to the FATF framework, some of the appropriate standards concerning regulation and supervision of financial institutions are those established by the Basel Committee, IOSCO, IAIS, and the International Accounting Standards Committee. The FATF framework would usually expect those standards to apply for monitoring compliance with the core AML measures for the types of institution/activity they cover. However, that may only be appropriate if the prudential supervisor is responsible for monitoring compliance with AML measures – which is not necessarily the case in all jurisdictions. There may also be other standards that evolve. However, making all of those prudential supervisory standards a mandatory requirement in the FATF 40 in all cases might not meet universal acceptance – although it is an option that could be adopted and which seems to be implied in the NCCT Criteria.

170. Another approach is for the revised FATF framework to contain some guidance to jurisdictions that outline the spectrum of regulatory options available and the factors that indicate the need for more intensive or less intensive regulation and supervision. However, if jurisdictions are provided with such a discretion they must be able to convince the FATF and its evaluators that the systems they have in place result in an effective and efficient anti-money laundering system for the financial sector. An approach based solely on guidance, while perhaps being more universally acceptable to many jurisdictions, could prove more problematic insofar as assessing compliance is concerned. For that reason, and because it moves away from what is already set out in the NCCT Criteria, it is unlikely to be a favoured option.

171. In summary the main options available regarding regulation and supervision would seem to be:

Option 1
All financial institutions covered by the FATF framework should be licensed or registered and should be supervised, including being subject to on-site inspections.

Option 2
Jurisdictions should put measures in place for all financial institutions to ensure that they are:

- Subject to legal or regulatory measures to guard against control or acquisition by criminal elements.

(The FATF invites comments on whether a less prescriptive approach on this element could be taken for certain types of financial institutions, which might be determined on a risk-based approach.)

- Subject to the AML measures;
- Complying with AML measures;
- Able to be prosecuted or otherwise sanctioned for non-compliance with AML measures.

Such measures must include:

- A registration or licensing regime for bureaux de change and money remitters;
- Powers to conduct on-site inspection or gain assurance from the likes of an auditor about compliance with AML measures.

In addition, any financial service providers that an international supervisory standard applies to should be licensed or registered and supervised in accordance with the applicable standard.

4. CORPORATE VEHICLES – BENEFICIAL OWNERSHIP AND CONTROL INFORMATION

172. The FATF has been concerned for several years about the availability of information on the persons that are the true owners and controllers of assets derived from criminal activity. Such persons have increasingly used various types of legal entities or arrangements to conceal their ill-gotten wealth, as part of the money laundering process.

173. Recommendation 11 already requires financial institutions to take reasonable steps to identify the persons on whose behalf an account is opened or a transaction conducted if there are doubts as to whether these customers are acting on their own behalf, and the Interpretative Note highlights the particular risks that might arise in relation to legal entities. This section considers the risks, the obligations that currently apply, the purposes for which beneficial ownership and control information should be required, and possible measures that could be taken. There are also specific sections that focus on the issues of bearer shares and trusts.

4.1. Beneficial ownership and control information generally

4.1.1. The problems and risks

174. This section of the paper considers the issues surrounding obtaining, accessing and sharing beneficial ownership and control information, and the need to consider amplifying the FATF Recommendations in their application to "corporate vehicles"[25], covering –

- Financial institutions and non-financial entities – when meeting their customer due diligence obligations: the need to be able to independently verify the identity of the beneficial owner, both when accounts are opened and subsequently during the relationship.
- Law Enforcement, FIU & Financial Regulators – timely availability of information on beneficial ownership to, and sharing of that information between investigators, FIU and regulators, both at national and international levels.

175. As stated in the OECD Report entitled "Behind the Corporate Veil - Using Corporate Vehicles for Illicit Purposes" issued in 2001 ("the OECD report") –

> "239. To successfully combat and prevent the misuse of corporate vehicles for illicit purposes, it is essential that all jurisdictions establish effective mechanisms that enable their authorities to obtain, on a timely basis, information on the beneficial ownership and control of corporate vehicles established in their own jurisdictions for the purpose of investigating illicit activities, fulfilling their regulatory/supervisory functions, and sharing such information with other authorities domestically and internationally."[26]

176. The FATF has consistently found that the lack of transparency concerning the ownership and control of corporate vehicles is a problem for money laundering investigations. For example, the FATF report on money laundering typologies issued in February 2000 states

[25] The terms "beneficial ownership" and "corporate vehicle" are defined in the Glossary to this Consultation Paper.

[26] p.41 of the OECD Report

"Legal entities or other types of types of legal relationships (such as trusts) formed by these professionals remain ubiquitous in money laundering schemes described by FATF members".

177. Similarly, when the FATF reviewed the criteria for defining non-cooperative jurisdictions, it found that:

> "Commercial laws, notably company formation and trust law, are of vital importance in the fight against money laundering. Such rules can hinder the prevention, detection and punishment of criminal activities. Shell corporations and nominees are widely used mechanisms to launder the proceeds from crime, particularly bribery (for example, to build up slush funds). The ability for competent authorities to obtain and share information regarding the identification of companies and their beneficial owner(s) is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering."[27]

178. Other recent studies have also noted the lack of transparency of corporate vehicles as being a matter of serious concern:

> (a) In March 2000, the T.M.C. Asser Instituut (in co-operation with the Ministry of Justice of the Netherlands and Europol) prepared a comparative study within EU Member States on the possibilities for the improvement of the international exchange of information on legal persons. The report found "that crime involving legal persons constitutes a serious problem that penetrates the public and legitimate private sector and threatens the transparency of (international) trade as well as that of society as a whole."
>
> The report recommended, inter alia, the need:
>
> "To take measures to make legal persons and the persons behind them more transparent. To make sure that the available databases that provide information on legal persons:
> 1. are up-to-date, reliable and on-line and generally accessible;
> 2. provide basic information about the legal person;
> 3. in addition, provide information about the natural persons who are 'behind' the legal person (directors, shareholders, beneficiary owners)."
>
> (b) In 2001, Transcrime prepared a study for the European Commission entitled "Transparency and Money Laundering". That study found that several types of corporate vehicles (public and private limited companies, trusts, and société de droit civil) are often used in money laundering operations, and that the lack of identification of the "real beneficial owner" was identified as a major problem for competent authorities and financial institutions, which need to identify the true owners and controllers of such vehicles.
>
> c) In 2002, the European Commission issued a report that noted that increased corporate transparency is required to combat financial abuses that threaten the integrity of the international financial system[28]. A recent Conference of European Union Parliaments

[27] see paragraph 19, report of the FATF on Non-Cooperative Countries or Territories issued on 14 February 2000

[28] see http://europa.eu.int/eur-lex/en/com/cnc/2002/com2002_0081en01.pdf

Against Money Laundering also issued a declaration calling for measures to be taken to improve the transparency of corporate vehicles.

179. The FATF has always recognised the importance of financial institutions, law enforcement authorities and FIUs, and financial regulators being able to obtain accurate information on the persons that are the ultimate beneficial owners or controllers of property, including property held in the name of legal entities. Recommendation 11 states that information should be obtained about the persons on whose behalf accounts are opened and transactions are conducted. This extends to information on the persons that are the principal owners and controllers of legal entities.

4.1.2. Corporate Vehicles

180. While this section of the Consultation Paper refers to the beneficiaries/controllers in respect of all corporate vehicles (the vehicles mentioned above are frequently interwoven in corporate structures) the issues surrounding the transparency of trusts are dealt with in more detail below, as is the issue of how to ascertain the beneficial owner of bearer shares (see sections 4.2. & 4.3. below). Also relevant to matters covered in this section of the paper is the section below on company and trust service providers (see section 5.3.).

181. Information on the beneficial ownership of corporate vehicles is required for a wide range of purposes. It is needed for –

- The prevention and control of money laundering and in particular the obligation of entities to report suspicious transactions.
- Suppressing the financing of terrorism, terrorist acts and terrorist organisations.
- The effective investigation/prosecution of criminal and civil cases.
- The effective exchange of information between regulatory and law enforcement authorities and FIU.
- The freezing and seizing of funds and other assets.
- Financial institutions and non-financial entities to undertake proper customer due diligence to minimise reputational and other risks.

Separate from the requirements for anti-money laundering and financial regulation purposes is the need of tax administrations for information on beneficial ownership.

182. Difficulties can arise in obtaining information on the beneficial owners of particular corporate vehicles that lend themselves to abuse through a lack of transparency (e.g. where companies can be incorporated without any disclosure of beneficial ownership). In the case of owners and controllers it is therefore important to ascertain the natural persons who ultimately lie behind the corporate vehicle. It is usual for those engaged in illegal activities to try to disguise and obscure their beneficial ownership of assets and make it more difficult for the enforcers of money laundering and regulatory legislation by creating a complex structure of companies and trusts, established in a number of different jurisdictions. It is important to

be able to get to the end of the chain. Experience has shown that this can seldom be achieved without full and effective co-operation among all the jurisdictions involved.

183. The essential requirements to be met (which are consistent with the fundamental objectives outlined in the OECD Report) are –

- The existence of adequate, accurate and timely information on the beneficial ownership of corporate vehicles which also reflects ongoing changes in that ownership.

- Proper oversight of the systems for maintaining or obtaining beneficial ownership and control information.

- Law enforcement and financial regulators should have the ability to obtain or access information on beneficial ownership in a timely fashion for the purposes referred to in paragraph 181 above.

- Financial institutions and other entities subject to customer due diligence obligations should be able to obtain timely information on beneficial ownership.

- The ability to share information on beneficial ownership with other law enforcement/regulatory authorities or FIU, both domestically and internationally.

Of these requirements the first is considered to be of the first order of importance, in that having legislation requiring beneficial ownership information to be held by banks, non-bank financial institutions, or professional intermediaries, and providing access to such information, is of little help if there is no, or only inadequate and inaccurate information is available. It also highlights the critical importance of effective customer due diligence procedures and controls being required of all entities that are subject to anti-money laundering and financial regulatory legislation.

184. There must be effective systems to ensure that the procedures in place for obtaining and monitoring information on beneficial ownership are applied effectively. In addition, and while recognising legitimate individual or business rights of privacy, there must be no absolute barriers, which prevent this information being obtained by the parties requiring access. There should also not be any laws, regulations or practices that prohibit or unduly restrict the sharing of such information with other regulatory/law enforcement authorities where there are legitimate regulatory or law enforcement requirements.

185. Information on beneficial ownership is important for –

- financial institutions and other entities for due diligence purposes;

- financial institutions and other entities for suspicious transaction reporting requirements;

- regulatory authorities to evaluate financial institutions' risk management systems; and

- law enforcement authorities and FIUs for investigations/prosecutions.

186. For the purposes of the FATF framework, the prime requirement is for financial institutions and the regulatory/law enforcement authorities to have timely access to accurate and meaningful beneficial ownership information when this is required. Whether such information should be recorded on a register, which can be accessed in some way by the "public", in order that they should know with whom they are dealing, and without prejudicing legitimate privacy interests, is a broader issue that is not the focus of the FATF. Most jurisdictions in which companies are incorporated require a public registry of companies, but in many cases the registry is not centralised, and will not contain beneficial ownership information.

4.1.3. "Risk Spectrum"

187. From the OECD report and other information it is apparent that, while almost any corporate vehicle is capable of being used for illegal purposes, some vehicles present a lesser risk and some a higher risk. There is a "risk spectrum", and factors that might indicate or affect the degree of risk are set out below.

188. The following factors, which are not listed by order of risk, are directly relevant[29] to the ability of (a) law enforcement and FIUs, (b) regulatory authorities, and (c) financial institutions and non-financial entities to obtain and/or access reliable information on the beneficial ownership and control of corporate vehicles. The factors should be considered having regard to the different types of corporate vehicles, and the degree of risk in a jurisdiction may be higher or lower depending on the laws and systems that exist for all these factors.

- Whether information concerning the beneficial ownership and control of a company is required to be recorded, maintained and kept up to date.

- Whether similar requirements apply concerning information on the settlor or founder, protector (where he exists), trustee and beneficiaries of a trust or foundation, and the partners of a partnership.

- Whether a regularly updated list of the shareholders, directors, and principal officers of all companies is required to be maintained.

- Whether all or some of this information is required to be maintained:
  a) on a public register;
  b) on a private register available to entities that are subject to customer due diligence requirements;
  c) on a private register available to regulators/law enforcement/FIU;
  d) by licensed/regulated trust and company service providers;
  e) by unregulated trust and company service providers;
  f) by the entities themselves.

[29] It should be recalled that there are also other factors that are not stated here, which go beyond the specific issue of beneficial ownership information, and which affect the overall effectiveness of an anti-money laundering system. These include the powers, functions and resources of the investigative and regulatory authorities, the scope of the criminal legislation, the preventive measures applicable to the financial or other sectors, the capability of a jurisdiction to co-operate internationally etc. The nature of all these measures and the whole anti-money laundering system also has an effect on the level of overall risk.

- Whether there is a register (public or otherwise) of the corporations, trusts, foundations and partnerships that are created, incorporated, registered or administered in the jurisdiction.

- Is the above information required to be maintained in (a) the jurisdiction of creation/incorporation, (b) the jurisdiction(s) of administration or operation {if different to (a)}, or (c) both (a) and (b).

- Are bearer or nominee shares allowed, and if so, is there an effective mechanism that will allow the ultimate beneficial owner of the shares to be ascertained.

- Are corporate or nominee directors allowed, and if so, is there an effective mechanism that will allow the natural person with ultimate control of the company to be ascertained.

- Is there a requirement that at least one director of the company/trustee of a trust/administrator of a foundation/partner in a partnership must be a natural person resident in the jurisdiction of creation/incorporation/administration.

- Whether corporate secrecy or privacy laws prevent or unduly restrict access to beneficial ownership information.

- Are financial institutions obliged to obtain beneficial ownership information, and perform customer due diligence when it commences, and during the course of, a business relationship, in particular when opening an account for a customer.

- Whether competent authorities have been designated to oversight and monitor compliance with the above requirements, including imposing sanctions for non-compliance where appropriate.

- Can law enforcement authorities and FIUs, and financial regulatory authorities, obtain or access beneficial ownership information on a timely basis: (a) for their own investigative or regulatory purposes, (b) based upon a legitimate request from a similar foreign authority, and share that information on a timely basis, and without unduly restrictive conditions.

189. In addition to the above factors, it must also be recognised that there are also specific types of corporate vehicles where information on beneficial ownership is likely to be of little if any relevance for anti-money laundering, and could be considered a lesser risk; for example -

- Occupational pension funds.
- Mutual funds and similar types of pooled investments.
- Entities owned or controlled by government or public authorities.

4.1.4. OECD Options for Obtaining and Sharing Information

190. Differences in legal and regulatory systems and practices, and the varying extent to which corporate vehicles are beneficially owned and controlled by residents or non-residents,

may mean that no one option is appropriate to all jurisdictions. However the key requirements outlined in paragraphs 181-183 should be met, whatever option is adopted. Also, as the OECD Report states, while jurisdictions may wish to rely mainly on one particular option it is unlikely that the objectives will be achieved without the jurisdiction implementing aspects of the other options.

191. The OECD Report identifies three possible options for obtaining beneficial ownership and control information –

- Option 1: Upfront disclosure to the authorities;
- Option 2: Requiring corporate service providers to obtain, verify and retain records on the beneficial ownership and control of corporate vehicles (the 'intermediary option');
- Option 3: Primary reliance on investigative measures when illicit activity is suspected;

and lists the primary advantages and disadvantages of each, their suitability and their important elements.

192. The primary advantages and disadvantages of each of the options in the OECD Report, as stated in that report, are as follows[30] –

Option 1: "an upfront disclosure system improves the transparency of corporate vehicles and ensures that certain authorities within a jurisdiction will, at all times, possess beneficial ownership and control information of corporate vehicles established in that jurisdiction. An upfront disclosure system may also enhance the capacity of jurisdictions, especially but not exclusively those with limited resources and weak investigative powers, to cooperate more rapidly and effectively with foreign authorities. In addition, an upfront disclosure system, if effective, may have a strong deterrent effect because individuals seeking to obscure their identity through the use of corporate vehicles are likely to go to a different jurisdiction where anonymity can be more easily achieved. An upfront disclosure system would also enable governments to make available beneficial ownership and control information to financial institutions (through various means such as a semi-public or public registry) in order to enhance the ability of these institutions to comply with their customer identification obligations, especially in the anti-money laundering context. However, in jurisdictions with a substantial domestic commercial sector, an extensive upfront disclosure system may, under certain circumstances, impose significant costs on corporate vehicles (particularly smaller enterprises)".

Option 2: "the 'intermediary option' may allow jurisdictions with limited financial and human resources to ensure that beneficial ownership and control of information is available within their jurisdictions without having to adopt a full-fledged upfront disclosure system. In addition to the upfront disclosure option, the intermediary option may be particularly appropriate for jurisdictions where persons connected to the corporate vehicle are typically not located within the jurisdiction of establishment and

[30] There may also be other advantages or disadvantages e.g. there may be timelags between the recording of beneficial ownership information and actual beneficial ownership at any particular point in time.

where the corporate service provider serves as the primary link to such corporate vehicles. Provided that corporate service providers are able to – and do – maintain the requisite information on corporate vehicles and the domestic authorities have the capacity to – and do – ensure compliance with the applicable requirements, an 'intermediary option' may also strike an appropriate balance between furthering the public's interest in combating the misuse of corporate vehicles and protecting legitimate privacy interests. Under certain circumstances, this mechanism may also have a preventive effect. Nonetheless, by requiring the authorities to obtain beneficial ownership and control information from third parties, the 'intermediary option' introduces the potential for delays in the provision of information."

Option 3: "For jurisdictions that have already developed an effective and efficient investigative mechanism, continued primary reliance on this mechanism may be more cost effective than to establish and maintain an extensive upfront disclosure system. Moreover, in jurisdictions where a substantial domestic commercial sector exists, primary reliance on an investigative mechanism may, under certain circumstance, avoid unnecessary costs or burdens on corporate vehicles (particularly smaller enterprises), which may stifle legitimate business formation. An investigative mechanism, if effective, may also enable policy makers to maintain a reasonable balance between ensuring proper monitoring/regulation of corporate vehicles and protecting legitimate privacy interests. An investigative system however, requires the authorities to obtain beneficial ownership and control information from third parties, thereby introducing the potential for delays in the provision of information."

193. It is arguable that no one option is sufficient in itself. The essential elements that should be present are, to repeat from paragraph 183 –

- The existence of adequate, accurate and timely information on the beneficial ownership of corporate vehicles which also reflects ongoing changes in that ownership.

- Proper oversight of the systems for maintaining or obtaining beneficial ownership and control information.

- Law enforcement and financial regulators should have the ability to obtain or access information on beneficial ownership in a timely fashion for the purposes referred to in paragraph 181 above.

- Financial institutions and other entities subject to customer due diligence obligations should be able to obtain timely information on beneficial ownership.

- The ability to share information on beneficial ownership with other law enforcement/regulatory authorities or FIU, both domestically and internationally.

These requirements are interrelated. A system based on option 1 will only be effective if there is proper oversight of the systems/procedures in the corporate vehicles/institutions supplying information to the authorities. A system based on option 2 must also provide for the obtaining and sharing of information by the authorities. A system based on option 3 will only be effective if there is accurate information available in the corporate vehicles/institutions that are the subject of investigation.

194. A key requirement concerning all of the options is an ability to ensure compliance. To quote from the OECD report –

- Option 1: "to be effective, it is important that the authorities are able to – and do – impose sanctions on corporate vehicles that do not comply with the applicable requirements under an upfront disclosure system."

- Option 2: "to be effective, it is essential that sanctions are imposed on corporate service providers and where appropriate, on corporate vehicles, that do not comply with the applicable requirements."

- Option 3: "the effectiveness of an investigative system depends, to a significant extent, on the likelihood that beneficial ownership and control information … is available within the jurisdiction in which the corporate vehicles were established. …[and] to enhance the capacity of authorities to obtain beneficial ownership and control information, a jurisdiction may choose to require companies to maintain such information."

4.1.5. Actions to remedy the areas of weakness

195. Having regard to the foregoing, the FATF is considering several complementary ways in which action could be taken to ensure that the agencies and entities referred to in paragraph 174 can obtain beneficial ownership and control information in a timely way, and whereby the key requirements in paragraphs 181-183 could be met:

A. Enhanced customer due diligence

Recommendations 10 and 11 presently set out the circumstances in which financial institutions should identify their customers, including taking reasonable measures to identify the beneficial owners. The measures being considered concerning the expansion and clarification of the customer due diligence requirements, will assist in identifying the beneficial owners of corporate vehicles. Some of the relevant measures being considered are:

- Financial institutions and non-financial businesses must be vigilant in preventing corporate vehicles from being abused by natural persons as a de facto method of operating anonymous accounts.

- There must be proper identification of the natural persons who are the ultimate beneficial owners, and financial institutions and non-financial businesses must have access to this information.

- Particular care should be taken when corporate vehicles have overly complex ownership structures that do not serve a legitimate purpose.

- Financial institutions and non-financial businesses should understand the structure and the purpose of the corporate vehicle, determine the source of funds and identify the natural person who are the ultimate beneficial owners, including those who have control of the funds.

- Particular care should be taken where the corporate vehicle is incorporated/administered in a jurisdiction that does not provide for a system that satisfies the requirements set out above.

B. Commercial law requirements

Requirements could be imposed in the commercial law field:

- Which ensure that all countries have laws and systems in place, and have adequate powers to ensure compliance with the key requirements set out in paragraph 183 of this paper. This could be based on the measures set out in the options for obtaining or accessing beneficial ownership and control information in "the OECD report". As noted in paragraph 193, a combination of measures would be necessary for this to be effective.

- That address those factors outlined in paragraph 188 above that most seriously lead to illicit use of corporate vehicles, which reduce transparency, and which introduce obstacles to the effective combat of money laundering. The papers dealing with bearer shares and trusts set out specific options, which provide solutions for dealing with the lack of or reduced transparency that may exist with respect to those instruments or arrangements.

C. Guidance

Guidance might be prepared which amplifies the "risk spectrum", and provides sound practice guidance in developing systems to obtain beneficial ownership information. This option would have to be prepared after there is a decision as to any minimum standards that might be agreed under the Recommendations.

4.2. Bearer Shares

196. Bearer shares confer rights of ownership to a company upon the physical holder of the share. They are commonly and legitimately used in a number of countries. However, the high level of anonymity they offer provides opportunities for misuse. In some countries, the identity of bearer shareholders is recorded or can be obtained by entities subject to customer due diligence obligations and the enforcement authorities. But, where the identity of the shareholder is not recorded when the share is issued and transferred or where it is not possible for the entities subject to customer due diligence obligations and enforcement authorities to obtain this information, ownership of the share is effectively anonymous. Such shares are open to two money laundering risks:

- financial assets can be acquired without the purchaser being identified;
- companies may be owned and controlled by interests who cannot be identified.

197. This has implications for FATF Recommendation 10, which requires financial institutions to identify clients when opening business relationships or conducting transactions. Recommendation 10 goes on to say that, when dealing with legal entities, financial institutions should take measures to verify the details of that entity, including the name of the customer. Recommendation 11 states that financial institutions should obtain information on the identity of beneficial owners, and expressly recognises the risks associated with domiciliary companies. The Interpretative Note to that Recommendation states that financial institutions should obtain information on the principal owners and beneficiaries of legal entities, either from a public register or from the client.

198. The FATF Recommendations say nothing specific about bearer shares, nor do they require any controls to be placed on their use. They are not specifically mentioned either in the 25 NCCT Criteria. However, in the June 2000 NCCT Report, the FATF set out five issues of particular concern. These included:

> "Difficulties in establishing the beneficial ownership of some legal entities, including companies issuing bearer shares and trusts."

199. This section analyses the extent to which bearer shares are a money laundering risk, considers their legitimate uses, and sets out a number of options for dealing with the risks. Other types of bearer instruments can be transferred anonymously, such as bearer bonds. Their transfer does not lead to the exercise of anonymous control of a company but bearer bonds pose some of the same risks involved in bearer shares: money laundering, fraud, theft, concealing assets. So, although this section of the paper concentrates on bearer shares, jurisdictions may wish to consider options for bearer bonds, which might also be applied to other types of bearer securities.

200. Bearer shares can be issued in companies that are listed on public stock exchanges and in non-listed companies. The money laundering risk of bearer shares in publicly listed companies is less than for non-listed companies, in respect of the danger that the company may be owned or controlled by unidentified interests. In publicly listed companies share ownership is likely to be diverse and there are laws in most countries requiring the identification to the company of any shareholding worth more than a small proportion of the voting rights. The same rules do not generally apply to shareholdings in non-listed companies and it is possible in some countries for such companies to be controlled by shareholders who

are effectively anonymous. Lower risks arise for money laundering in relation to companies that are publicly traded on a regulated market. There are also other substantial arguments why the options being considered for bearer shares should not be applied to such companies. The FATF seeks comments on this issue.

201. The risk that financial assets can be acquired without identification of the purchaser remains for all bearer shares, regardless of the nature of the company. Indeed this risk applies to all bearer instruments.

4.2.1. What are Bearer Shares

202. The OECD Report of April 2001 on Using Corporate Entities for Illicit Purposes defined bearer shares in the following terms: "Bearer shares are negotiable instruments that accord ownership of a corporation to the person who possesses the bearer share certificate. In other words, the who has physical possession of the bearer share certificate is deemed to be the lawful shareholder of the corporation …and is entitled to all of the rights of a shareholder".

4.2.2. The Purpose of Bearer Shares

203. Their central feature is ease of transfer of ownership. This convenience is the reason why they are an important part of the ownership of companies in several countries. As an example, the box below describes in more detail the arrangements for issuing and holding them in Switzerland.

4.2.3. The Purpose of the Bearer Share

Example:
In an FATF member country, public companies can choose to issue registered or bearer shares. Registered and bearer shares may also coexist in a proportion stipulated in the statutes of the company.

In practice, it is often the case that when founding a company, the founders secure control with the help of registered shares, while a further circle of investors receive bearer shares.

Family businesses also often make use of this possibility: the family shareholders are allowed registered shares with restricted transferability of low nominal value and the public is offered bearer shares with high nominal value. Only the bearer shares are quoted on the stock market.

The coexistence of registered shares with restricted transferability and bearer shares has often been used until now in order to safeguard national control of a company: Only citizens were allowed as registered shareholders whereas bearer shares were available to everybody. A new stock corporation law put into force at the beginning of the 1990s greatly restricted this possibility. Furthermore, in recent years there has been a shift towards ordinary shares, which is primarily conceived as a registered share with weakly restricted transferability.

4.2.4. Advantages of Bearer Shares

.

204. There are a number of **legitimate** reasons for permitting bearer shares.

- **Quick, easy and cheap control**: A corporate vehicle is formed to handle an international transaction involving a number of business people in the transformation of a product, with higher levels of value added at each stage. In order to obtain credit from their financiers, each business person holds the entire value of the product at that stage by virtue of the bearer share that is passed to them when they accept the product for further transformation. For example, a high-pressure vessel for the oil refining industry, originally made in Country A and then finished in Countries B, C and D before being delivered to the customer in Country E. A company with limited liability can be created within seconds through a global network of agents and intermediaries, often using internet-based company incorporation systems, for as little as US$100. There are limited minimum capital reserve, due diligence or reporting requirements for such companies.

- **Concern about the competition:** Privately-held or closed companies, or non-listed public companies that are popular in Europe, operate in a fiercely competitive market. Many companies are structured to maintain flexibility in the control and transfer of ownership of one's company and to restrict the availability of commercial information pertaining to the company. Closed companies may issue bearer shares to restrict the flow of commercially sensitive information by keeping to themselves information about their activities and their profits. For example, a company in jurisdiction A found a low cost source of processed shrimp in jurisdiction B and sold it into established markets in Europe. They concealed their interests in the deal by establishing a company from jurisdiction C and handing the bearer shares to an intermediary in jurisdiction D. The intermediary could demonstrate ownership of the company through custody of the bearer shares and act as the principal in the deal with financiers on behalf of the partners in jurisdiction A. Once the deal was concluded they recovered the bearer shares from the intermediary.

- **Demand for security by financiers:** One-off business transactions often use IBCs with bearer shares to securitise the deal. For example, a financial group in jurisdiction W agreed to provide trade finance on a transaction involving a textile contract between a supplier in jurisdiction X, an intermediary in jurisdiction Y and a customer in the jurisdiction Z. The only security available for the financial group was in the goods making up the consignment. The intermediary formed an IBC with bearer shares that were held by the financial as collateral against the trade finance. In the circumstances of any default all the goods would have clearly belonged to the financier.

Another example where bearer shares might secure finance for a business transaction is where a bank lent money to a customer for the purchase of a commercial trading vessel. In addition to seeking a charge against the company and a mortgage secured against the ship, the bank insisted that it hold bearer shares in order to prevent the company created for the deal from taking on any other financial liabilities that might rank ahead of their claim, in the event of bankruptcy.

4.2.5. Scope for Abuse of Bearer Shares

205. There are other reasons for using bearer shares which particularly concern law enforcement authorities and financial regulators:

- **Privacy of ownership:** Corporations have legitimate reasons for maintaining the privacy of their ownership in certain instances, as described above. But such privacy has other consequences. For example, if there is no legal requirement for the company secretary or registered agent to register and keep up to date details of the beneficial ownership of bearer shares, or subsequent transfer of ownership of those shares, it is impossible for a potential creditor to identify whether assets are available to satisfy a court judgement. In such cases, bearer shares can be used to hide ownership of assets to avoid financial responsibility and court judgements in favour of creditors or to pay spousal or child support following marriage breakdown. They can also be used to hide the ownership of assets and the identity of owners from the tax authorities.

- **Drugs, Arms and other Illegal Activities:** Criminals have grown adept at using intermediaries (lawyers, accountants and company formation agents) to create networks of companies to channel illegal funds through. Those funds may be the proceeds of crime, or may provide the financing for further criminal activity. If customer due diligence systems are operating effectively, it should be possible for entities to identify companies that seek to conduct business with them by identifying the shareholders and beneficiaries, and the nature of the company's business.

206. Companies formed in this way may also be used to purchase property with illegal funds, or to hold assets on behalf of other individuals or companies. The ability to purchase land or property through such corporate vehicles should normally involve a lawyer or estate agent subject to customer due diligence rules. Again, anti-money laundering systems are only as strong as the weakest point. If there are barriers to establishing the beneficial owner of a company, entities will not be able to know their customers, and loopholes will emerge.

207. Bearer shares are not the only reason why financial institutions may have difficulty identifying the beneficial owner of companies (nominee shareholdings or holding assets through trusts can create difficulties). But, a financial institution dealing with a company whose shareholdings are entirely or mainly in pure bearer form faces an almost impossible task in identifying beneficial ownership. Not only is the information not recorded, but there may be no corporate agent with that information. Indeed company directors may not know who currently holds the bearer shares and therefore owns the company.

4.2.6. Examples of the Misuse of Bearer Shares

Example 1:
Several subjects were arrested following a parallel drug and proceeds of crime investigation by Jurisdiction A into an international organisation engaged in the massive importation of hashish into Jurisdiction A and another jurisdiction. As a result of these arrests, information was received regarding the world-wide operations of the group and more specifically how they laundered their illicit profits in Jurisdiction A. A subsequent search of a residence in Jurisdiction A, revealed that the registered owner of the residence was a corporation registered in Jurisdiction B. During the course of the search of the house, several bearer share certificates were seized which were attributable to several other corporations in Jurisdiction B, including the corporation to which the residence being searched was registered. Inquiries through the Land Titles in Jurisdiction A revealed two other properties, which were registered to the corporations in Jurisdiction B and linked to the bearer share certificates.

Official Requests were made to the Government of Jurisdiction B for legal assistance in determining the beneficial owners of the corporations but despite protracted negotiations, the corporate information was never released. Links between the corporations in Jurisdiction B and a member of the criminal organisation being investigated in Jurisdiction A were made through correspondence located in Jurisdiction A. This clearly established beneficial ownership. It is quite apparent that if this correspondence had not been located in Jurisdiction A it would have been impossible to link the two entities. The three properties previously mentioned were valued at over $4.5 million (Can) and were subsequently forfeited.

Example 2:

As a result of a drug importation investigation, approximately CAD2.75 million was restrained in combined assets from residential property and bank accounts. These assets were located in two North American countries and two European countries. Significant assets restrained involved two offshore companies incorporated in Jurisdiction A. Investigators also seized original bearer shares of three offshore companies and original articles of incorporation. The investigation revealed that one of the suspects used the services of a lawyer from Jurisdiction B to design a money laundering scheme, which included the corporation of offshore companies with bearer shares. The lawyer hired the services of a management company in Jurisdiction C, who in turn used the services of a company in Jurisdiction A to incorporate bearer share companies in Jurisdiction A and Jurisdiction D.

There was absolutely no requirement to register the names of the shareholders at the corporate registry office, company head office or anywhere else. The only names that appear are the original incorporators of the company in Jurisdiction A, who then forwarded the bearer shares and articles of incorporation to the management company.

The management company then forwarded the original bearer shares and articles of incorporation to the Jurisdiction B lawyer, who in turn handed them over to the client. The files held by the management only contained the names of the nominee directors, nominee administrators and the direction given by the Jurisdiction B lawyer who acted on behalf of the suspect shareholder.

The use of bearer share companies and professional intermediaries in this investigation almost offered absolute anonymity to the natural person in possession of the bearer shares and is clearly a powerful tool to conceal proceeds of crime. If investigators had not seized the bearer shares in the possession of the suspect, it would have been impossible to determine the owner of these companies and ultimately to identify and restrain their assets as proceeds of crime. In this case, the offshore companies held significant assets alleged to be the proceeds of crime, bank accounts in Jurisdiction C, and residential property in Jurisdiction B & E.

4.2.7. How could bearer shares be controlled

Bearer Shares in one FATF member

An FATF country has two methods for transferring bearer shares:

Bearer shares represented by physical titles. In this case, the person to whom a bearer share is initially handed and all the subsequent changes of ownership are known because the creation and the transmission of the bearer share must be conducted through a notary or licensed financial institution. These intermediaries are obliged to collaborate with the competent judicial authorities as well as with the competent authorities on the fight against money laundering.

Bearer shares represented by book entry shares. In this case, shares must be registered. The register has to be held by a security agency or company. The subsequent changes of ownership being registered in every moment, the real owner of the bearer share is always identified.

208. A number of ways of ensuring that bearer shares are not used for criminal purposes including money laundering are set out below. Which, if any of these options are chosen by a jurisdiction, will depend upon a judgement of whether the costs of such measures are proportionate to the threat of money laundering through abuse by corporate vehicles which issue such shares. However, the objective of any of the options is to ensure that entities subject to customer due diligence requirements, law enforcement authorities and FIUs, and regulators are able to obtain accurate information on the persons that are the ultimate beneficial owners or controllers of property, including property held in the name of legal entities. Lower risks arise for money laundering in relation to companies that are publicly traded on a regulated market. There are also other substantial arguments why the options being considered for bearer shares should not be applied to such companies. Different solutions may also be appropriate for other types of anonymous securities such as bearer bonds.

209. An overall consideration for section 4 is that the revised FATF Recommendations will have to reflect a balance in terms of the measures applied to different types of corporate vehicles. Three options for consideration for jurisdictions that permit bearer shares are:

a) **Central Registration - All bearer shares should be registered centrally** with details of the owner and physical location of the shares kept on a company registry in the jurisdiction of incorporation. Transfers of shares should be recorded and notified to the registry at the time of that transfer. Company registrars must be obliged to provide details to the competent authorities, subject to appropriate due process. This requirement should be strengthened by providing that unless this is done, shareholder rights such as voting rights or the receipt of dividends could not be exercised. Shareholders would be required to identify themselves when they sought to exercise such rights. Such a requirement would effectively convert bearer shares into registered shares, effectively eliminating pure bearer shares. As shares are increasingly “dematerialised” with the increased use of electronic shareholding and

dealing, bearer shares in publicly listed companies are likely to disappear. However, while dematerialisation of shares in publicly listed companies is likely to grow, it will probably not do so for private or public companies whose shares are not listed on a stock exchange. These, of course, are the companies where there is the biggest risk of exposure to money laundering.

b) **Bearer shares should be immobilised.** The share certificates could be physically deposited and held by a "custodian" who is a licensed financial institution in an FATF jurisdiction, or a jurisdiction that meets FATF standards.

c) **Information about the natural persons who are the ultimate beneficial owners of bearer shareholdings, or at a minimum those shareholdings that control the company, must be maintained or be obtainable by law enforcement authorities and FIUs, regulators and entities subject to customer due diligence requirements.** The precise mechanism by which this is achieved could be left to each jurisdiction to determine. Amongst the possible approaches to meet this requirement are:

(i) The company should be required to maintain this information and make it available for inspection by the authorities on request. If this information is available within the company this would also allow entities subject to customer due diligence requirements to verify the beneficial owners of bearer shareholdings, or at a minimum those shareholdings that control the company.

(ii) The company should be required to file certain information with the Registrar of Companies. As a minimum, this could be the name and address of the business, names and addresses of those authorised to make financial commitments on behalf of the company (e.g. board members, directors, authorised representatives).

(iii) As per option (ii), but there would also be an obligation to file the names and addresses of those with shareholdings above a certain threshold percentage.

(iv) The creation and subsequent transfer of all bearer shares would have to be carried out or authorised by a public official or a financial service provider/institution or non-financial business that is subject to the FATF framework. This would be conditional upon a number of steps being taken to strengthen transparency of beneficial ownership including:

(a) proper identification and recording of the parties involved when the bearer share is acquired, obtained or transferred.
(b) the notification of the company of the acquisition or transfer and the power to exercise ownership rights (e.g. voting rights, right to transfer the share and/or receipt of dividends) being conditional upon these steps being done.

210. There are advantages and disadvantages to each option. The first option clearly deals with the risks associated with bearer shares, but also removes the advantages they offer to legitimate users. The second option maintains some of the flexibility offered by bearer shares, although the requirement to use licensed entities to immobilise them would increase the costs

of making such transfers. The various alternatives in the third option would allow for easy transfer of ownership but carry with them risks that, if the institution responsible for keeping records did not do so and bearer shares were misused, all the rights to the shares could be exercised unlawfully without detection.

4.2.8. A Menu or Minimum Standards

211. Finally, a possible approach to the issue might be for the FATF not to make any of these options as mandatory but set out some or all of them as a "menu" and invite countries to choose which to apply, according to the circumstances prevailing in their jurisdiction. It would be mandatory to do something from the menu and the jurisdiction would need to demonstrate in mutual evaluations etc, its compliance with the FATF standard on bearer shares, and that it had chosen an option that dealt effectively with the money laundering risks associated with bearer shares in that jurisdiction. This is similar to the approach in the OECD Report. It is a rather different approach, though, from the one normally adopted by FATF, which is to set minimum standards and leave it to individual countries to adopt more significant measures if they consider this necessary.

4.3. Trusts

212. Trusts[31] are an integral part of the jurisprudence of many nations throughout the world. They are part of legal systems that enable people (and judicial authorities) to resolve many difficult problems of a personal nature (e.g. in relation to succession planning, provision for family members and others in a structured and legally binding way, protecting beneficiaries against their own weaknesses, bringing together in a cohesive whole assets dispersed throughout the world and entrusting assets to professional management on a long term basis). Trusts also play a major role in commercial transactions (such as securitisations) and in such socially beneficial areas as pension schemes, employee benefit schemes and legitimate charities.

213. In many jurisdictions trusts are not improper. Many trusts are formed for everyday legitimate purposes for inheritance, the education of minors, recognised registered charities etc. which pose little risk of money laundering. However it is not possible to identify separate categories of trusts that will be entirely free of concern. Rather what is required, and what this paper is designed to do, is to identify the characteristics of trusts that are able or are perceived to present risks of money laundering, and propose practical options for eliminating or minimising such risks. In presenting the options however it is recognised that the circumstances pertaining in individual jurisdictions will call for some flexibility in translating the options into practical action.

214. A trust is not a legal entity. It is a description of a relationship wherein the trustee is the legal owner of assets, having had them vested in them by the settlor, and acts in the interests of another person – the beneficiary, or for a specified purpose. Trusts are normally created in writing in a "trust deed" or "trust instrument", and these are commonly referred to as express trusts. Certain specific types of trust relationships, such as constructive or resulting trusts, are not created in writing, and arise by law. A trust company is a company whose business is acting as a trust or company service provider. It forms and administers trusts and companies and arranges for the appointment of trustees. Trust services can be provided by a range of entities and individuals. They can be performed by trust companies. They are often performed by lawyers and accountants, and they are sometimes performed by individuals or partnerships[32].

215. Whilst acknowledging their legitimate use in business and their long tradition in several jurisdictions, trusts like companies and bank accounts can be misused. Such misuse has been identified in recent reports such as the OECD Report on Using Corporate Vehicles for Illicit Purposes, the UN Report on Offshore Financial Centres and the Transcrime Report for the European Commission on "Transparency and Money Laundering". There is a need to find a means of coping efficiently with this misuse without damaging the legitimate use of trusts. This can be achieved by enhancing the level of transparency of trusts in general, since transparency is the most effective deterrent in preventing misuse of trusts, companies or bank accounts. Transparency is important in ensuring that law enforcement and regulatory authorities can have access to information when required. Transparency also allows entities to

[31] As noted in section 4.1 above, the FATF is also concerned about the potential misuse of foundations. Foundations are entities that have certain features in common with trusts, and the FATF intends to consider the types of measures that may be required to prevent them being misused.
[32] For background information on the types of trust see Annex 5.

undertake effective customer due diligence without which business relationships should not be established.

4.3.1. What can give rise to insufficient transparency

216. Aspects of some trusts that can give rise to lack of transparency and enable their misuse, which are also to be found in the misuse of companies, limited partnerships and other legal entities, can be itemised as follows –

a) Trusts can exist without any written record. These conditions, where they exist, can create difficulties for law enforcement or regulatory authorities (either administrative or judiciary) to gather rapidly information or evidence regarding the very existence of the trust and collect the names of their settlor and beneficiary(ies). In such circumstances, it can also be very difficult, if not impossible, for an entity carrying out customer due diligence to know and verify the name of a beneficiary of a financial transaction conducted through such a trust.

b) A trust deed can exist which does not identify the settlor and/or the beneficiary. Together with the situation in (a) above, this can create an important obstacle for the law enforcement authorities to identify rapidly the beneficiary(ies) of the trust, and can hamper an entity in fulfilling properly its customer due diligence requirements.

c) Some forms of trusts, such as the discretionary trust, can make it possible to give the trustee discretionary power to name the beneficiary within a class of beneficiaries and distribute accordingly the assets held in trust. The beneficiary can be named or changed at any time, which can make it possible to keep the beneficiaries' identity secret up until the time the ownership of the assets held in trust is transferred to them. As in (a) above, this can also make it difficult, if not impossible, for an entity to know and verify the name of a beneficiary of a financial transaction conducted through such trusts.

d) The laws of certain jurisdictions have encouraged the development of so-called asset protection trusts which can protect the settlor from the freezing, seizure or confiscation of the assets, even though the settlor is able to keep control over their management, either by giving the trustee instructions or by naming a protector. In some jurisdictions, the settlor can be made a beneficiary of the trust without anyone being able to find out.

e) Decisions about the management of trusts may not be recorded and they may not be disclosed in writing to anyone. If such decisions are not recorded at least by the trustee the law enforcement authorities cannot have access to them.

f) Trusts can be set up for the purpose of managing shares in a company, which can make it even more difficult to determine who the true beneficiaries of assets managed by companies are (cascade arrangements). These kind of arrangements often have the purpose of hiding the identity of the ultimate beneficiary(ies) or real owner of an asset.

g) Flee clauses can constitute an obstacle to an effective anti-money laundering framework, in particular in terms of international legal assistance. These clauses

permit the automatic change of the law of the trust in case of certain events. With such clauses, it is possible to protect trust assets against legal action.

h) In some countries, the use of trusts can be a way to escape from judicial decisions that freeze, seize or confiscate the assets located in trusts. Some legislation can explicitly prohibit the freezing, seizure or confiscation of the assets located in trusts.

4.3.2. The Objective and Minimum Requirements

217. In seeking to enhance the transparency of trusts it is not the intention to limit the proper use of trusts, or to deny that some aspects of a trust that can give rise to misuse also support the legitimate uses to which trusts can be put. The objective is to prevent trusts from being used to:

- circumvent the money laundering prevention laws (especially the customer due diligence procedures);
- frustrate domestic and international investigations by law enforcement, FIU or regulators.

This objective is not peculiar to trusts. It applies equally to the misuse of other types of corporate vehicles or legal entities.

218. In seeking to achieve the above objective the following requirements need to be met:

- information about the identity of the settlor, trustee, possible protector and the beneficiary(ies) of a trust is available to entities when carrying out customer due diligence, and is accurate;
- the identity of the settlor, trustee, possible protector and the beneficiary(ies) of a trust is available on a timely basis to administrative or judicial law enforcement authorities or FIU, both at the domestic and international level, and is accurate;
- the affairs of a trust are properly documented and are available to law enforcement authorities in support of an investigation/prosecution.

4.3.3. Action to be Taken to Enhance the Transparency of Trusts

219. Trusts in common with other corporate vehicles can be misused for illicit purposes but their potential for such mischief can be better controlled through comprehensive and robust regulatory regimes, the abolition of secrecy provisions, ending the misuse or inappropriate reliance on privilege or confidentiality by professional gatekeepers such as lawyers and accountants, further requirements for financial institutions, the existence of appropriate gateways for the exchange of information and a capacity and willingness to co-operate on the part of regulators, intelligence agencies, law enforcement agencies and judicial authorities in line with international standards.

220. These requirements can be considered under the three following themes:

- Enhancing the level of transparency of trusts (reducing their opacity and the number of opportunities they offer to money launderers).

- Enforcing the trustees obligations and regulating trust and company service providers.
- Ensuring access by entities and relevant authorities to the relevant and accurate information about settlors, trustees, protectors and beneficiaries.

221. To help achieve these key objectives a number of possible measures can be considered. The first set of measures contains actions that reflect current practice in a number of jurisdictions, and which, subject to proper account being taken of differences in the legal systems of individual jurisdictions, provide examples of ways in which the options set out in section 4.3.4. below could be implemented. Subparagraphs (a) to (e) below are illustrative of the controls that could apply to company and trust service providers, and should be read in conjunction with the specific options noted in section 5.4.

a) Jurisdictions could introduce meaningful and effective legislation for the regulation and supervision of those involved in the business of providing trust and company services. All such businesses should be licensed. Only those who are "fit and proper" (in terms of integrity, competence and solvency) should be granted licences. It should be a criminal offence to provide trust and company services without a licence.

b) The regulator of the trust and company service providers could be a statutory regulatory authority, which should have the power to impose sanctions. As part of the licensing process, the regulator should carry out "on-site" inspection visits to observe at first hand and monitor the business, policies and procedures, etc. of the applicant. Meetings should take place with the directors and with members of staff selected at random. The inspection visit should also include an examination of client files.

c) If the applicant is regarded as "fit and proper", and is therefore awarded a licence, there should be further on-site inspection visits at regular intervals to monitor whether the licensee continues to operate the business in an acceptable manner. A particular focus of all "on-site" inspection visits should be to verify whether those engaged in the provision of trust and corporate services comply fully with all aspects of customer due diligence (customer verification, keeping of records, training of staff, recognition and reporting of suspicious customers/transactions). The regulator should be legally entitled to view all files and documents.

d) All necessary information relating to customers of service providers (including the names of beneficial owners and controllers of companies and the trust deed with the names of the settlors, protectors, trustees and beneficiaries of trusts, etc) should be maintained in the jurisdiction and be accessible to regulators, law enforcement authorities, FIU as well as entities which need such information to undertake effective customer due diligence. There should be specific provisions in legislation or codes of good practice on the obligations placed on trust service providers covering customer identification, "letters of wishes", specification of assets held in the trust, documentation of asset management decisions etc.

e) All trust and company service providers should be subject to anti-money laundering legislation including the making of suspicious transaction reports. They should be responsible for knowing the identity of those who are the instigators and

beneficiaries of a trust and for the ongoing monitoring and documentation of the affairs of a trust.

f) There should be measures in place to ensure that all relevant information relating to a trust can be exchanged in an effective manner between law enforcement, regulatory, and other competent authorities, both within a jurisdiction and internationally.

g) All jurisdictions from which trust or company products are offered, or in which trusts or companies are administered, should ensure that there are laws in place which set out clearly the respective responsibilities of trustees, company directors and others involved in the management and control of such entities.

h) The setting up of so-called "charitable trusts" with no named individuals as beneficiaries should be monitored – and thereby their misuse discouraged – by requiring full details of such trusts (including any letters of wishes) to be provided to the relevant authority.

i) Entities opening accounts in respect of trusts and companies should be required to identify the ultimate beneficiary(ies) and principal(s) of such structures in accordance with customer due diligence standards to the same extent as if applications were being made by individuals to open personal accounts. Limited exceptions should be permitted in respect of unborn and infant beneficiaries. Limited exceptions should be permitted in respect of large classes of beneficiaries (particularly if the interests of some of them are only contingent and somewhat remote) but "client identification" and verification of such individuals should be required before any payments are permitted from the account to them. Entities are not under any legal compulsion to open an account if they are not satisfied with information supplied to them in relation to customer identification, and they should have procedures in place to deal with situations where they are not totally satisfied. As noted at paragraph 33, these procedures could include not opening an account, preventing withdrawals from the account, or filing an STR.

222. A second set of possible measures that could be considered have not been as widely adopted, although some of the measures have been adopted in certain countries. These measures include:

a). Full and Proper Documentation - it is a reasonable general proposition that all trusts should be fully and properly documented. For example, at the time the trust is created, this might require a written trust deed, setting out the names of the settlor, trustee, beneficiary, protector, property covered by trust, real object etc., together with an obligation to subsequently update this information. However there are some cases, where, for example, it only becomes apparent retrospectively that a trust exists e.g. a court decides that there is a constructive trust (see Annex 5). In those cases, it would not be possible to objectively know that the trust existed until that time, and thus it could not be documented in advance.

Where trust and company service providers act in relation to trusts they should do so only in relation to trusts that are fully documented. As far as constructive trusts are concerned, the details of beneficial ownership and effective control would normally

become fully transparent as part of a court's decision, and thus be available to the relevant parties.

b). Discretionary Trusts - the trust deed should set out the information referred to above, and this should be verified by the trustee (in the same manner as a bank collects and verifies the identity of its customer). The use of discretionary trusts should be restricted in order to enable the proper identification of all the possible beneficiary(ies).

Some flexibility is required to address the situation where circumstances might change over time (e.g. the birth of children and the increasing incidence of successive marriages and divorces, and the necessity of providing for children and dependants of previous marriages whether of one of the original beneficiaries or a partner), but the requirement should then be that those providing trust services should at all times be able to identify the known beneficiaries. To balance the uncertainty accepted by the financial institutions managing the accounts of these trusts, the trust service providers should be required to inform the financial institutions when changes in beneficiaries do occur, although specific exceptions may be needed for certain types of trust where beneficiaries fall into a class and the costs of notifying each change was excessive e.g. a charitable trust established by a government authority creating and then maintaining a public park where the beneficiaries might be expressed as all of the citizens residing in a geographic area.

c). Register - the trust deed (with all relevant information) should be registered in a register held by a competent authority. There could be several options as to the degree of access that is accorded to some or all the information on the register. Entities that have to perform customer due diligence should have timely access to this register as should administrative and judicial authorities for the purpose of their administrative or judicial investigations.

There are arguments in favour of and against a register of trusts. Those who favour this proposal argue that it would assist entities in fulfilling their customer due diligence and reporting requirements. However, institutions would often be able to access information more directly from their customer, which would be more comprehensive and up-to-date than that which would be on a register, though the institution would be reliant on the customer for the accuracy of the information. In addition, entities should not accept a customer unless all the information required for effective customer due diligence is obtained.

A register, it is suggested, would allow administrative and judicial authorities, including FIU, readier access to key information for fighting money laundering and regulating the financial system. However the information on a register would not be sufficient in itself. Access to a register could need to be restricted to reconcile the need to protect legitimate privacy needs and existing legitimate privacy laws with the needs for improving the fight against money laundering and to deter the use of trusts to obscure individuals' identities. A failure to update information contained in the register would need to constitute an offence, for the accuracy of the information provided, to be ensured. Careful consideration will need to be given to comparing the benefits that might be obtained from a register and comparing them with the costs that would be incurred.

d). Prohibition of, or restrictions on "charitable trusts" without named individuals as beneficiaries and on trusts having another trust as beneficiary.

So called "charitable trusts" are capable of misuse but there are also many legitimate "charitable trusts" and it would be detrimental to the charities concerned if they were not to be permitted. The key point is to ensure that one can discover the real beneficiary underlying a trust.

e). Prohibition of "flee clauses" - The concern for "flee clauses" arises where the purpose of such a clause is to engage in "jurisdiction hopping" and thereby make it difficult for anyone to challenge the trust effectively or otherwise to litigate effectively. On the other hand a "flee clause" can be used to provide for the proper law of the trust to change automatically upon the happening of certain events, such as a revolution or invasion or other event associated with civil unrest and political instability. This provision is only effective if the trust is governed by the proper law of one jurisdiction, while the assets are held in another. The elimination of "flee clauses" would not be of any concern to any politically stable jurisdiction involved in quality business but, given the many reasons for the formation of trusts and the many eventualities to be provided for, it could be argued that rather than prohibit "flee clauses", their use should be restricted to avoid misuse and constraints to international co-operation. Thus, an appropriate compromise might be to restrict the use of "flee clauses" to a number of defined legitimate circumstances, such as those mentioned above.

4.3.4. Options to Consider

223. An overall consideration for section 4 is that the revised FATF Recommendations will have to reflect a balance in terms of the measures applied to different types of corporate vehicles. There is a reasonable degree of common ground that in order to ensure the transparency of trusts certain minimum standards must be applied to them i.e.:

- the existence of adequate, accurate and timely information;
- proper oversight of systems for maintaining or obtaining information;
- timely access to information by law enforcement and regulatory authorities and FIU;
- financial institutions and other entities subject to customer due diligence obligations should be able to obtain timely information on beneficial ownership;
- the ability to share information with other law enforcement and regulatory authorities, and FIU, both domestically and internationally.

224. The issue is how to achieve such transparency in practice. A range of options have been proposed but they basically divide into three broad approaches, which are broadly similar to the approaches set out in the OECD Report in which "corporate vehicles" is defined to include trusts and foundations. A system based on option 1 below will only be fully effective if there is proper oversight of the system/procedures in the institution supplying information into the authorities. A system based on option 2 must also provide for the obtaining and sharing of information by the authorities. A system based on option 3 would only be effective if there is accurate, accessible and up to date information available at the legal entity being investigated or at a related financial institution. All options require that information about the trustees, beneficiaries and settlors must be maintained, be obtainable or could be subject to

timely disclosure for law enforcement, regulators, FIU, and financial institutions and entities subject to customer due diligence obligations.

225. As the options for obtaining beneficial ownership and control information are to a large degree complementary, jurisdictions that rely primarily on one particular option may, depending on their particular circumstances, find it highly desirable and beneficial to supplement this mechanism with other options. (Executive summary of OECD Report "Behind the Corporate Veil"). The options are:

Option 1
Upfront disclosure to the authorities of information on:

- the name of the trust and trustees; or
- as above **plus** the name of the settlor, protector and the beneficiaries or class of beneficiaries; or
- as above plus the trust deed.

This amounts to registration of trusts. There are also options as to whether the register should be one kept by the authorities and whether it contains information that should be disclosed to the public.

Option 1a
The register would be public. This would provide financial institutions and other entities subject to AML requirements, including customer due diligence obligations, with a source of information to help them effectively discharge these obligations.

Option 1b
However, some information about the beneficiaries of trusts, and even their existence, often contains detailed personal information whose disclosure could seriously affect personal privacy. It may therefore be considered preferable to restrict public access to this information and limit it to law enforcement and regulatory agencies, and FIU.

Whatever the decision on access, it would have to be understood that such a requirement could only apply in practice to explicitly formed trusts and not to constructive trust relationships, which are incapable of such registration. To be effective the authority or body which registered trusts would need to have powers of oversight over the suppliers of such information to check that the criteria in paragraph 221 were being complied with. There would also need to be powers for the authorities to share such information with their overseas counterparts.

Option 2
Requirement for anyone involved in the establishment or management of trusts on a professional basis to obtain, verify and retain records on the settlor, beneficiaries (or class of beneficiaries) and controllers such as trustees or protectors as part of:

- anti money laundering legislation; and/or
- the application of a regulatory regime to all trust and company service providers.

There would also need to be powers for the authorities to share such information with their overseas counterparts.

Option 3

Reliance on investigative powers when illicit activity is suspected. The authorities would need to have powers to compel the provision of information about the settlor, protectors and beneficiaries of trusts to law enforcement and, as appropriate, regulatory authorities. These authorities would also need to have power to share such information with their overseas counterparts.

5. NON-FINANCIAL BUSINESSES AND PROFESSIONS

226. The FATF Forty Recommendations already contain several recommendations that apply to businesses and professions that are not financial institutions. Recommendation 9 asks countries to consider applying Recommendations 10-21, and 23 to the financial activities (as defined in the Annex) of non-financial businesses or professions. In addition, Recommendation 27 requires the designation of competent authorities to supervise and regulate the implementation of the Recommendations in professions that deal in cash.

227. Currently, more than two-thirds of FATF members have applied some or all of the anti-money laundering measures contained in Recommendations 10-21 to persons or entities other than financial institutions. The second EU AML Directive, amending the 1991 directive, was adopted on 4 December 2001, and now applies anti-money laundering obligations to several additional classes of businesses and professions:

- Auditors, external accountants, and tax advisors.
- Real estate agents.
- Casinos.
- Dealers in high value goods, e.g. precious stones or metals or works of art, when there is a payment of € 15,000 or more in cash.
- Notaries and other independent legal professionals - when they participate in planning certain types of transactions for their clients, or if they act on behalf of and for their clients in any financial or real estate transaction.

228. EU member states have until 15 June 2003 to transpose the new Directive into national law. It extends the anti-money laundering obligations, in particular the requirement to identify customers and the obligation to report any fact which might be an indication of money laundering, to a series of non-financial businesses and professions.

229. For several years FATF Typologies reports have referred to the increasing role played by professional service providers and non-financial businesses in money laundering schemes. For example, the 2001 Typologies Report states:

> "Lawyers, notaries, accountants and other professionals offering financial advice have become the common elements to complex money laundering schemes. This trend is mentioned by almost all FATF members."

230. The money laundering risks associated with such businesses and professions have also been expressly recognised by the European Commission, the European Parliament, and the United Nations. The 1998 United Nations report entitled "Financial Havens, Banking Secrecy and Money Laundering" states –

> "Money launderers frequently use lawyers and accountants to help them hide funds. All too frequently, unscrupulous lawyers provide advice on money-laundering to their clients on the assumption that they will be protected by the rules of privilege that protect the confidentiality of the lawyer/client relationship."
>
> and

> "Gambling casinos have been used to hide the proceeds of drug sales for more than 50 years. Casinos are ideal vehicles for laundering because they generate large amounts of unaccounted for cash… Because of the vulnerability of casinos to money-laundering operations, it is essential that the industry be more carefully regulated".

231. Taking these significant risks into account, the FATF is therefore considering extending the application of Recommendations 10-21 and 26-29 to seven types of non-financial businesses or professions. Those seven categories are:

- Casinos and other gambling businesses
- Dealers in real estate and high value items
- Company and trust service providers
- Lawyers
- Notaries
- Accountants and auditors
- Investment advisors

232. For each category of business or profession, the paper focuses on the options for several key issues that would be relevant to the application of an anti-money laundering system:

(a) a more precise description of the businesses or professions, and the activities to be covered;
(b) customer due diligence rules;
(c) suspicious transaction reporting and increased diligence; and
(d) regulation and supervision.

233. For certain businesses or professions, it might also be possible to consider alternative or additional options (see paragraph 10 above). In addition, except where explicitly provided for e.g. professional secrecy obligations, a necessary component of all systems would be that there are no secrecy laws, regulations or rules that prevent the various businesses or professions from providing the relevant information or making it available to law enforcement or regulatory authorities when they have legitimate inquiries. Similarly, the laws must provide the necessary gateways for exchange of information internationally, and must not prevent or unduly restrict the flow of such information.

234. Consideration should also be given to the interaction between the earlier sections of the paper, particularly section 3, and this section. If AML obligations are widened, clarified or amended pursuant to the discussion in earlier sections, this could have an impact on the proposals and options in section 5.

5.1. Casinos and other gambling businesses

235. This section of the paper discusses casinos[33] and other types of gambling activity and their vulnerability to money laundering, briefly examines the anti-money laundering measures taken by some jurisdictions, and sets out some options. Estimates of the size of the gambling industry precisely are sizeable. For example, a 1999 US report[34] found that the annual revenues for various types of casino gambling exceeded USD 26 billion, revenues for horse race betting were approximately USD 3.25 billion, and estimates of illegal sports betting ranged from USD 80-380 billion. A UK study[35] found that the annual gambling turnover in 1998 in the United Kingdom was approximately GBP 42 billion, of which nearly half was casino gambling, and rest principally horse racing, gaming machines and the national lottery.

236. Recent studies of internet gambling suggest that while this form of gambling may still be relatively small, it is growing rapidly. Internet gambling refers to both Internet betting[36] and Internet gaming[37]. The issue of the vulnerability of Internet gambling, which is closely linked to the broader issue of the risks that arise from electronic financial services, is one that the FATF recently considered. The 2001 Typologies Report states – "Internet gambling might be an ideal web-based "service" to serve as a cover for a money laundering scheme through the net. There is evidence in some FATF jurisdictions that criminals are using the Internet gambling industry to commit crime and to launder the proceeds of crime."

5.1.1. Casinos: Vulnerability to Money Laundering

237. Casinos are vulnerable to manipulation by money launderers due to the fast-paced and cash intensive nature of the games and because casinos provide their customers with a wide array of financial services. Financial services available at casinos are similar and, in many cases, identical to those generally provided by banks and other depository institutions and can include customer deposit or credit accounts, facilities for transmitting and receiving funds transfers directly from other institutions, and cheque cashing and currency exchange services.

238. The experience of law enforcement and regulatory officials suggests that the gambling environment often attracts criminal elements involved in a variety of illicit activities, including fraud, narcotics trafficking and money laundering. With large volumes of currency being brought in and played by legitimate customers, gaming can create a good "cover" for money launderers who are in possession of large amounts of currency. Casinos are also attractive to organised crime if the criminals are able to take over and control the casino, thus

[33] This paper takes the definitions used by the UK Gambling Review (see below). A casino is a commercial gaming club that provides table games other than bingo, but may also provide other types of gambling e.g. gaming machines (a game of chance machine, which requires coins or tokens to be activated).

[34] The report can be located at http://www.ngisc.gov/reports/fullrpt.html

[35] The report of the Gambling Review can be found at http://www.gamblingreview.gov.uk/

[36] Internet betting is making bets using the internet as a conduit to place a bet. The gambling event takes place off-line and the result is independently verifiable i.e. the on-line system does not generate the result, it is used simply for communicating information. The internet is often an alternative to other means of entry to the gambling venue such as the post or telephone.

[37] Internet gaming is on-line gaming where the gambling event takes place via the internet and is probably based on a random number generator. The games may appear as virtual-casino style games, slot machine games or interactive lotteries.

providing them with an opportunity to launder their illicit proceeds, as well as engage in other types of criminality. The FATF has consistently noted the use of casinos in money laundering schemes in its annual Typologies Reports, while those countries that require casinos to report suspicious transactions have received significant numbers of STRs.

239. The money laundering schemes that have been uncovered include instances in which casinos were used by individuals to commit offences including structuring and money laundering, many of them involving organized crime. Also, money launderers have been known to use agents to disguise the true ownership of the funds and are willing to lose some of the money while gambling as a necessary cost of doing business. Other techniques include:

- Buying chips or tokens with cash, conduct minimal betting and then request repayment by a cheque drawn on the casino's account.
- Using a chain of casinos with establishments in different countries and asking for the amount held by the casino in credit for gambler to be made available in another jurisdiction and then withdraw it in the form of a cheque there.
- Asking for winner's cheques to be made out in the name of third persons or without a nominee.

5.1.2. Detection of Suspicious Casino Transactions

240. In most casinos, officials monitor the gaming activity of customers, usually to ensure that there is proper gambling conduct, rather than as a measure to combat money laundering. However, these officials, together with employees who conduct transactions with a customer are in a unique position to recognise transactions and activities that appear to have no legitimate purpose, are not usual for a specific player or type of players, or are not consistent with transactions involving wagering. This is because while suspicious transactions and activities can take place anywhere in a casino, they usually occur at a casino cage, gaming table or slot machine.

241. It is not necessary that currency be involved in the transaction for it to be considered suspicious. Sometimes the transactions will be in the form of monetary instruments, wire transfers or credit cards in which the initial placement of illegal proceeds may have occurred at a financial institution or a series of financial institutions. At times customers and/or agents are willing to lose a nominal amount of chips by making small bets or offsetting larger bets and then exchanging the chips for currency, a check or a wire transfer. Suspicious activities often involve structuring to avoid record-keeping or reporting thresholds, using agents to conduct multiple transactions for an anonymous individual, transacting large amounts of funds with little or no related gaming activity (*i.e.*, false drop), providing false documents or identifying information, and layering transactions to disguise their source.

242. The suspicious nature of the transaction may first be detected by an employee conducting the transaction, a supervisor observing the transaction, or a surveillance department employee monitoring the transaction. In certain instances, there may be facts and circumstances along with the casino's knowledge of its customer, which provide a reasonable explanation for the transaction that would remove it from the suspicious category.

243. There may be any number of reasons why a transaction, under particular facts and circumstances, is suspicious. In addition, the suspicious nature of transactions is cumulative in its effect. The more frequently any one or combination of these examples occurs at a casino,

the more likely it is that the customers conducting these transactions are committing, or may be attempting to commit, financial crimes. The scrutiny needed to identify suspicious transactions highlights the importance of casinos knowing their customers.

244. A casino must know its customer to make an informed decision as to whether a transaction is suspicious. Many casinos already know a great deal about their customers from information routinely obtained through deposit, credit, cheque cashing and player rating accounts. These accounts generally require casinos to obtain basic identification information about the accountholders and to inquire into the kinds of wagering activities in which the customer is likely to engage. For example, deposit and credit accounts track customer deposits and casino extensions of credit. The player rating account tracks gaming activity and is designed primarily to award complimentary perquisites to volume players, and to serve as a marketing tool to identify frequent customers and to encourage continued patronage. In certain instances, casinos use credit bureaux to verify information obtained from customers. All of these sources of information can help a casino to understand better its customer base and to evaluate specific transactions that appear to lack justification or otherwise cannot be explained as falling within the usual methods of legitimate business.

5.1.3. Non Casino Gambling: vulnerabilities to money laundering

245. Other than casinos the more prevalent forms of legal gambling include horse racing betting (on and off course), slot and other gaming machines, soccer and other types of sports betting, spread betting, card clubs, and lotteries and pool competitions. Some of these other types of gambling provide an ideal cover for money launderers because they have a high volume cash turnover, offer considerable anonymity for customers, no recognisable audit trail and persons that engage in significant gambling are usually welcome. The vulnerabilities identified above for casinos are equally applicable to some other forms of gambling. In addition, in some jurisdictions gambling businesses such as betting shops, card clubs and off-course bookmakers are vulnerable to money laundering because they provide services similar to financial institutions, including customer deposit, or credit accounts, facilities for transmitting and receiving funds from other financial institutions, cheque cashing and currency exchange.

246. Gambling is particularly attractive to money launderers at the placement stage. Sale of winning horse-racing tickets has been identified in money laundering cases, with the criminal buying winning tickets with criminal proceeds and then obtaining a cheque when the winning ticket is returned. There is evidence that telephone betting accounts have been abused by launderers as both a means of disguising who is really gambling and also legitimising funds; cash is paid into such accounts, a small amount is gambled and the balance transferred back out into a bank account. The bank then records the source of the funds as winnings thereby lessening suspicion.

247. Gambling businesses that use a token or chip system such as poker machines, are also vulnerable to money laundering. Any chip system that permits a customer to purchase chips with funds, which can then be sold back, provides a low cost, intensive opportunity for structuring and conversion of funds.

248. Historically organised crime and other criminal elements have always been attracted to gambling. The combination of large profits, cash transactions and the opportunity to launder funds attracts criminal operators. The large amounts of cash introduced daily by legitimate

customers provide cover for money launderers without necessarily alerting the authorities. It is necessary that the gambling industry is aware of these risks and takes steps whether by regulation or otherwise to establish systems to counter them.

5.1.4. The measures currently in place

249. At a national level, a number of FATF members have required various types of gambling businesses to comply with anti-money laundering obligations, and casinos are generally tightly regulated and supervised, and usually subject to anti-money laundering requirements. In Australia and New Zealand, casinos, gambling houses and bookmakers who open accounts for customers are required to obtain identification before the account can be operated, as well as for all large cash transactions and any suspicious transaction[38]. There is also a requirement to report suspicious transactions, and implement other measures to combat money laundering. Similar requirements apply in the United States for casinos and card clubs. In Hong Kong, certain voluntary measures are in place. Customer identification and suspicious transaction reporting obligations apply in Brazil, Iceland and Turkey to lotteries, and in Finland to casinos, horse racing, lotteries and betting agents where the amount of the bet is over € 3000. Portugal has legislation requiring betting and lottery agencies to identity the holders of winning coupons and retain the relevant data for a 10 year period.

250. The EU Directive now extends to casinos, which are required to identify their customer by means of supporting evidence where gambling chips worth € 1000 or more are bought or sold. For casinos subject to state supervision this requirement is deemed to be complied with if their customers are registered and identified on entry to the casino. Where money laundering is suspected, the casino must identify the customer regardless of the amount involved, and is also obliged to file an STR with the competent authority. They are obliged to implement internal control measures and train their staff concerning money laundering issues.

251. In most jurisdictions, casinos and some other gaming entities are subject to some type of licensing or registration, regulation and supervision because of their vulnerability to various forms of criminal activity including money laundering, illegal betting, race or game fixing etc. However governments have regulated such businesses for other reasons as well, such as the need to ensure that gamblers receive fair treatment when gambling, and to protect persons that are potentially vulnerable. In certain jurisdictions, casinos are indirectly owned by the government, while in others private ownership is allowed, but usually on the basis of fairly strict licensing requirements. Where there is private ownership, a tight regulatory regime is intended to protect customers and ensure that the casino does not fall within the ownership or control of criminals or their associates. In addition, there are usually extensive checks on casino owners and operators. In some jurisdictions, casinos and certain other gambling entities have fit and proper tests for senior management, screening programmes for senior staff, and various compliance and training programmes.

5.1.5. Customer due diligence/ Record-keeping/Suspicious transaction reporting

252. The corner stone of an effective AML regime includes, as with other financial institutions, adequate know your customer and record keeping requirements and an effective suspicious transaction reporting regime. A casino or gambling business must know its

[38] In New Zealand casinos and gambling houses are the same thing and the "bookmaker" is a government owned and controlled entity.

customer before it can make an informed decision as to whether a transaction is suspicious. Most FATF members already require customer identification and record keeping by casinos, and a number of jurisdictions have extended these requirements to other gambling institutions. It may also be necessary to consider some minimum transaction threshold for the large numbers of occasional gamblers, i.e. persons that do not establish some type of account with the casino.

253. A further option would be for countries to extend the customer due diligence and record keeping measures to other gaming entities that are recognised within their jurisdiction as being vulnerable to money laundering. Many other such gambling entities already require identification before a substantial bet can be placed and carry out credit and identification checks on regular or high volume customers. Individual jurisdictions could set a threshold for the application of such measures appropriate to their own anti-money laundering regime. Records retained for the purpose of customer profiling and marketing would also provide information on customer betting patterns. Records of transactions and customers should be retained for a minimum period of 5 years in order that funds can be traced effectively and information made available to the regulatory and law enforcement authorities. Records should be retained in a format that can be used in judicial proceedings.

Options for coverage of gambling businesses

1. Businesses and activities to be covered

Given the proven risks that exist for the casino industry, and the high degree of regulation and anti-money laundering measures already in place, anti-money laundering measures should be made mandatory for casinos, and consideration should be given to tight anti-money laundering controls and supervision for casinos. As a minimum this should apply where the casino is an actual physical location, and consideration needs to be given to the practical application of anti-money laundering measures to Internet entities that provide similar gaming facilities.

Option 1- Casinos and a minimum set of other vulnerable gambling entities.

Option 2 – Casinos and other gambling entities that are perceived by each jurisdiction to be vulnerable to money laundering.

2. Customer due diligence

Option 1- For all customers whenever they (a) enter into a permanent or ongoing business relationship with the gambling entity, and (b) if they conduct a business transaction, purchase or sell gambling tokens or cash in winning tickets above a certain threshold. Given the diversity of gambling patterns between jurisdictions the threshold could be left to individual countries, though consideration might also be given to applying whatever standard may be agreed for financial institutions having large cash transactions with occasional customers (see section 3.6.3. above).

Option 2- For all customers as above but only when there are cash transactions above a certain threshold. Cash transactions would include withdrawals as well as deposits and currency exchange.

Option 3 – Apply requirements similar to those in article 3 of the EU Directive to casinos. The Directive allows for some discretion when the entity is state supervised.

It is proposed that the standard set out in Recommendation 12 should apply to all three options, namely, retain records of transactions and customers for a minimum period of 5 years.

3. Suspicious transaction reporting and increased diligence

Option 1 – Mandatory for any suspicious transaction, regardless of the amount of money involved.

Option 2 – Mandatory for casinos to report all suspicious transactions, but other types of gambling entities that are covered by AML obligations need only report suspicious transactions exceeding a certain threshold.

Whichever option is adopted, Recommendations 14 and 16-19, which lay out other measures that are required for additional diligence should also apply.
Countries should issue guidelines on suspicious transactions that reflect the nature of gambling within their own jurisdictions.

4. Regulation and supervision

Casinos

Casinos should be fully regulated and supervised, while each jurisdiction could apply such measures to other gambling entities as it deems necessary. Casinos should be subject, whether publicly or privately owned, to a regulatory and supervisory regime, consistent with each jurisdiction's anti money laundering policy, that ensures that they have effectively implemented the necessary anti-money laundering measures. In particular, stringent checks should be conducted on the owners, beneficial owners, managers and operators of casinos. Given that casinos are for the most part already regulated, this should not impose a disproportionate burden on the regulatory authorities.

Other gambling entities

Option 1 – jurisdictions could apply regulatory or supervisory measures, similar to those applicable to casinos, to other gambling entities as it deems necessary.

Option 2 – Jurisdictions could require other gambling entities to be subject to some form of self-regulation.

Option 3 – Jurisdictions could require the external auditors of gambling entities other than casinos to examine and report on the AML controls as part of an annual audit of the accounts of the entity.

5. Additional counter-measures for Internet gambling

The FATF will consider the application of appropriate AML counter-measures (similar to those outlined above) to effectively prevent misuse of internet gambling facilities by money launderers. This would also include consideration of several options that were suggested in the FATF 2001 Typologies Report:

1. Require Internet service providers (ISPs) to maintain reliable subscriber registers with appropriate identification information.
2. Require ISPs to establish log files with traffic data relating Internet-protocol number to subscriber and to telephone number used in the connection.
3. Require that this information be maintained for a reasonable period.
4. Ensure that this information may be made available internationally in a timely manner when conducting criminal investigations.

6. Other possible measures

1. Consider the circumstances and conditions under which casinos can offer various financial services, e.g. if casinos are allowed to operate like banks, what controls should be in place.

2. (a) Prevent casino chains being allowed to offer credit to clients at different locations without each individually conducting appropriate customer identification requirements?
   (b) This could apply either to all such situations or only to casinos operating in different jurisdictions.
   (c) Prevent casinos from allowing their chips to be removed from the casino premises.

3. Where a customer deposits cash when commencing their gambling activity, any winnings should only be returned to them as cash and in the same currency.

5.2. Real Estate Agents and Dealers in High Value Goods

254. Businesses and activities linked to trading in real estate and high value goods[39], which may be used in the placement or integration phases of money laundering, have been specifically identified as vulnerable to money laundering. For example, a recent FATF study of money laundering methods, techniques and trends found - "The real estate sector is now fully within the sphere of money laundering activities. Investment of illicit capital in real estate is a classic and proven method of laundering dirty money… Numerous cases of laundering were cited by the experts." Also "sellers of high-value objects like artworks are unquestionably a significant presence in laundering activities"[40].

255. Gold dealers have also been identified as being vulnerable to money laundering: "Several members reported that the vulnerability to money laundering within their countries has increasingly centred on specialised gold bullion sellers. This is due in part to the fact that anti-money laundering legislation targeting traditional financial institutions has generally caused those customers desiring to purchase bullion anonymously to turn to other sources"[41]. The 1998-99 Typologies Report also identified close links between wholesale and retail dealing in gold, informal remittance systems, and money laundering cases. Similar links have also been found between money laundering and trade in diamonds. More recently, these industries have been linked to the financing of terrorist organisations and activities.

256. In a number of FATF and other countries, there has also been extensive use of luxury vehicles such as expensive automobiles, and boats or planes, as part of the money laundering process. Such items are used both at the placement level, as a means of transporting cash or other criminal proceeds, as well as at the layering and integration stages, when they are luxury items that criminals own as part of their assets. Another type of business that is subject to anti-money laundering obligations in several countries and which is involved in transporting cash and high value items are professional carriers of cash and other valuables.

257. In considering the application of anti-money laundering measures to the real estate industry and dealers in high value goods, one must take into account that these industries may vary considerably in their types of clients, and the types and value of transactions that they conduct. However, they are quite similar in that they are generally not subject to any supervision or monitoring, except perhaps to a limited extent by professional bodies for some industries. Some practical difficulties might therefore arise in applying anti-money laundering measures to such businesses and activities, mainly due to this traditional lack of specific regulation of such businesses or control by a supervisory authority.

The measures currently in place

258. At a national level, relatively few FATF members currently require real estate agents or other dealers in high value items to comply with anti-money laundering obligations. Some examples include:

[39] The reference to "real estate agents" extends to those persons that are engaged in the business of acting as professional intermediaries in the purchase and sale of real estate for third parties. This could cover not just agents, but also brokers.

[40] FATF Report on Money Laundering Typologies 1997-98

[41] FATF Report on Money Laundering Typologies 1998-99

- Australia - gold dealers are treated in the same way as financial institutions and must identify their customers, keep records, report suspicious transaction, and implement other measures to combat money laundering.
- Spain – anti-money laundering requirements apply to individuals or legal entities that engage in: (a) real estate promotion or the buying and selling of real property, and (b) trade in precious gems, stones and metals and trade in art objects and antiques.
- Portugal applies its anti-money legislation to a similar range of businesses, as well as to dealers in cars, boats and aircraft, but only for cash transactions exceeding a certain size.

Certain AML measures also apply to a range of such businesses in other FATF countries – Argentina, Belgium, Brazil, Canada, Finland, Italy, Turkey and the United States.

259. The Directive, article 2a(6), provides that it now applies to:

> "6. Dealers in high-value goods, such as precious stones or metals, or works of art, auctioneers, whenever payment is made in cash, and in an amount of EUR 15 000 or more;"

Such businesses are also obliged to report suspicious transactions and implement internal control measures and train their staff concerning money laundering issues.

Options for coverage of dealers in real estate and high value items

1. Businesses and activities to be covered

Real estate agents, together with:

Option 1 – An agreed minimum list of dealers in high value items e.g. dealers in precious stones or metals, or in works of art or auctioneers.

Option 2 – Such other dealers in high value items as are perceived by each jurisdiction to be vulnerable to money laundering.

Option 3 – Option 1 or 2, but only if it involves cash transactions (including multiple linked transactions) exceeding a certain threshold e.g. USD/€ 15,000.

Where feasible, the FATF will seek to ensure consistency in any thresholds that are set, thus the threshold set above could be the standard that may be agreed for financial institutions having large transactions with occasional customers (see section 3.6.3.).

2. Customer Due Diligence

The options that are reasonably applicable concerning the verification of customer's identity may vary according to the type of business that is covered, and depending on whether there is an ongoing business relationship or whether it is a one-off transaction. Certain businesses, such as dealing in residential real estate or selling jewellery are more likely to involve one-off

transactions, while others, for example wholesale trading in precious metals or stones or dealing in industrial/office real estate, might be more likely to involve an ongoing relationship.

The businesses referred to above shall:

Option 1 – Carry out due diligence in respect of clients and/or the parties to the contract [and the object of any transaction], regardless of the means of payment employed.

Option 2 – Carry out due diligence in respect of clients and/or the parties to the contract [and the object of any transaction], whenever they exceed a certain threshold, which could be standardised (for example USD/€15000), or might vary according to the activity involved.

Option 3 – as set forth in Option 2 but only for transactions settled in cash.

Consideration also needs to be given as to whether one or more of the options would be more applicable to ongoing business relationships, while another option might be more appropriate for one-off transactions. It is also proposed that the standard set out in Recommendation 12 should apply, namely, retain records of transactions and customers for a minimum period of 5 years.

3. Suspicious transaction reporting and increased diligence

Option 1 – Mandatory for any suspicious transaction, regardless of the amount of money involved.

Option 2 – Mandatory only for transactions exceeding a certain threshold.

Whichever option is adopted, Recommendations 14 and 16-19, which lay out other measures that are required for additional diligence should also apply.

4. Regulation and supervision

The question of regulation and supervision raises a number of sub-issues.

(a) The means by which the authorities can determine whether there are businesses which are subject to the anti-money laundering obligations.
Different options could be applied to different categories of business, and the principal options are:

Option 1 - Rules or laws permitting or restricting activities being in place, and persons must declare/register involvement in activities (the name of the entity is added to a list and the entity is allowed to carry out activities, no discretion to reject application).

Option 2 - Rules or laws permitting or restricting activities being in place, and licenses are issued to conduct that type of business (the entity is evaluated against criteria by a competent authority and is allowed to carry out the particular activities).

(b) Oversight and supervision of compliance

Option 1 – To require the external auditors of high value dealers to examine and report on the anti-money laundering controls as part of an annual audit of the accounts of the entity.

Option 2 – Oversight by a self-regulatory organisation (SRO).

Option 3 – Oversight or supervision by one or more designated competent authorities (part of government). There could either be a single authority for all businesses and activities, or different authorities according to the activity.

The relevant body would need to have the appropriate powers to conduct assessments of whether a business is meeting its obligations.

(c) Sanctions system

The system should allow for sanctions for failing to comply with the relevant obligations. Those sanctions should be broadly proportionate and consistent with sanctions applicable to financial entities in similar circumstances. They could be criminal sanctions, administrative sanctions, or both criminal and administrative sanctions.

5. Other possible measures

1. Although there are potentially significant ramifications, a measure which has been adopted in some countries (three FATF members have such measures) is to impose a limit on the size of cash transactions. An option would therefore be to extend FATF Recommendation 24 by requiring any transaction above a certain threshold to be made by a payment method other than cash.

In considering this option, the FATF will consider very carefully the benefits to be obtained from implementing this option against the likely costs to society, including the risk of interference with the fundamental rights and liberties of individuals.

5.3. Trust and Company Service Providers

260. As is noted elsewhere, the FATF has consistently found that legal entities or other types of legal relationships (such as trusts), usually formed and managed by professional service providers are a common feature of money laundering schemes. A major part of the problem is the lack of transparency concerning the beneficial ownership and control of corporate vehicles such as companies, trusts, foundations etc., but an equally important issue is addressing the risks posed by the professionals that create and manage these vehicles.

261. It is important to have a good understanding of the relevant concepts and entities that are relevant to the industry. The concept and basis for a company is well known in all jurisdictions, but trusts are a concept that is less universal. A trust is not a legal entity. It cannot have a bank account and it does not own property. It is a description of a relationship wherein the trustee is the legal owner of assets, having acquired them from the settlor but acts in the interests of another person, the beneficiary.

262. There are a wide range of different types of businesses or professionals that act as professional service providers for the creation and administration of companies, trusts, foundations or other legal entities or arrangements. For example, in many jurisdictions, lawyers and accountants play an important role in this type of business, but the service is also provided by banks, businesses that specialise in providing these services or suitably qualified individuals or partnerships. The same term can also have different meanings in different jurisdictions. In some jurisdictions, a trust company is a company whose business is acting as a trust service provider, i.e. it forms and administers trusts and arranges for the appointment of or acts as trustees. In others, a trust company may also be entitled to do banking business, or to provide similar services with respect to companies. What counts for anti-money laundering purposes is not the name of business that provides the service but the types of service it provides. The services that could be covered are:

- acting as a company or partnership formation agent;
- acting as (or arranging for another person to act as) a director or secretary of a company or a partner of a partnership;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or for any other person;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

5.3.1. The money laundering risks

263. Companies and trusts are often used by money launderers and other criminals who wish to conceal their identity. For example, as stated in the 2001 Typologies Report, FATF experts found that "trusts, along with various forms of corporate entities, are increasingly perceived as an important element of large-scale or complex money laundering schemes". Because of this, it is important to ensure that those who are responsible for forming and administering trusts and companies must themselves, know the identity of the persons who are the beneficiaries or beneficial owners respectively, and who effectively control the trust or company in question. In 2000, the FATF examined the role of the individuals or agents that help to create such entities, and found them to be a key factor in an increasing number of complex money laundering schemes.

264. The need to take action with respect to trust and company service providers has also been recognised by other international bodies. The OECD Report highlights the role that trust and company service providers can play in the misuse of corporate vehicles. The identified misuse is not restricted to money laundering, but extends to bribery and corruption, hiding assets from legitimate creditors and claimants, fraud, securities law and tax offences. The report states:

> "76. Corporate service providers regularly design structures to ensure that the beneficial owner remains anonymous, and often act as the intermediary between the client and the authorities in the jurisdiction of incorporation.....
> 78. Trustees may also play a role in obscuring the identity of the beneficial owner....."

265. The Basel CDD paper also identifies client accounts opened by professional intermediaries as a high-risk area. These concerns have caused the Offshore Group of Banking Supervisors to set up a working group made up of members of the Group and representatives from several other countries and relevant international organisations. This group is working to produce a recommended statement of minimum standards and/or guidance for trust and company service providers.

266. The risks associated with "gatekeepers" have also been recognised by the G8. Following the meeting of Justice Ministers in Moscow in 1999, the official communiqué noted that many money-laundering schemes involve misuse of financial intermediaries. The Ministers noted that they would "consider requiring or enhancing suspicious transaction reporting by the "gatekeepers" to the international financial system, including company formation agents, accountants, auditors and lawyers ..."

267. When considering the options for addressing these risks, it is important to bear in mind the need for a level playing field, and the displacement effect that occurs when measures are taken in one jurisdiction but not in another. In relation to trust and company service providers, there is evidence that service providers relocate from jurisdictions that have adopt strong anti-money laundering and regulatory measures to those that have no such measures. Another important general consideration is that trust and company service providers often control large amounts of client funds and can make investment decisions for the trusts and companies that they control, thus acting in a comparable way to investment or portfolio managers. This has implications for anti-money laundering controls, but also for protection of customers against criminal activity or incompetence by the service provider.

5.3.2. The measures currently in place

268. In most FATF members trust and company service providers are not dealt with as a class of business that is subject to AML obligations. Rather, certain professions, such as lawyers or accountants, which commonly provide services such as creation and management of trusts and companies, are covered by the relevant obligations (as noted elsewhere in this paper). This concept is incorporated in the new EU Directive, in that notaries and lawyers fall within the scope of the Directive when they are acting in the exercise of their professional activities in relation to, inter alia, the "creation, operation or management of trusts, companies or similar structures".

269. However, in a number of jurisdictions outside the FATF, a much more comprehensive approach has been taken. Trust and company service providers are regarded as a part of the financial services industry and the sector is regulated and supervised in the same manner as investment business, banks, collective investment funds etc. In those jurisdictions, it was considered appropriate to insist that the same high standards of integrity, competence and financial standing should be applied to this sector as to other regulated financial sectors. The fact that trust and company service providers have another role, that of gatekeeper to the financial services sector, was another important reason for regulating the sector so as to protect the integrity of the system. Even where the service provider does not handle client funds directly, the service provider (like an investment advisor) often occupies a central and knowledgeable role with respect to a client's affairs – a factor of considerable importance in complex money laundering investigations.

270. The OECD Report also recognises that a full regulatory system for service providers could be necessary if a jurisdiction intends to rely on the service providers to obtain and record information on beneficial ownership and control of corporate vehicles. In most jurisdictions where service providers are comprehensively regulated, the same approach is taken for both trust service providers and company service providers, but a small number of jurisdictions apply stricter obligations to trust service providers.

271. The full regulatory approach that has been adopted in those jurisdictions usually deals with a number of key issues, which address not only money laundering concerns, but also consumer/customer protection, prudential concerns, the integrity of the system as a whole etc. The major issues that would be dealt with include:

- The fit and properness of those engaged in the provision of trust and company services and their business methods.
- The adequacy of the resources available to the service providers and the regulatory and law enforcement authorities.
- The availability of accurate, timely information, particularly on ultimate beneficial ownership.
- Adequate arrangements to share or exchange information.
- Adequate measures to protect customers and clients.
- Effective independent vetting and inspection arrangements.
- Ensuring directors and trustees exercise their responsibilities appropriately.
- Maintaining a high standard record keeping and auditing.

Options for coverage of trust and company service providers

1. Business or profession to be covered by anti-money laundering obligations

Option 1 - All businesses or persons that, as a commercial undertaking, provide services to third parties relating to the creation, management, administration or operation of companies, trusts, foundations or other similar vehicles should be subject to AML obligations.

Option 2 – the same as option 1, except that the AML measures would only apply where the service provider is involved in financial transactions with the client.

Where particular classes of professionals, in particular lawyers or accountants, are subject to some or all of the FATF Recommendations in respect of all or certain parts of their professional activity, there will be a need to ensure that the obligations imposed are consistent.

It may be however that jurisdictions believe that only some of the services or parts of the sector fall into a higher risk category and thus need to be subject to obligations. A further exception, applicable to both options, might therefore be to exclude service providers from coverage in relation to services such as merely forming companies, where control changes hands and there is no further involvement by the service provider. It might be argued that these activities are lower risk, and that application of the full set of anti-money laundering obligations is not necessary.

2. Customer due diligence

Service providers should be subject to the same customer due diligence as apply to financial institutions i.e. Recommendations 10 and 11 would apply. It is also proposed that the standard set out in Recommendation 12 should apply, namely, retain records of transactions and customers for a minimum period of 5 years.

3. Suspicious transaction reporting and increased diligence

The general principle should be that trust and company service providers would be obliged to comply with Recommendations 14-19, and in particular the reporting of suspicious transactions (though note the discussion in section 3.7.3.4. of reporting suspicious activity).

If the service provider is a lawyer, notary, accountant or auditor then the obligation to report a suspicious transaction may depend on any applicable professional secrecy or legal professional privilege (see the relevant section in the options for those professions for a more precise description).

4. Anti-money laundering regulation and supervision

As the provision of trust or company services is performed by several different types of professions or businesses, and the legislative action that has been taken at a national level varies widely, there is no uniform position concerning the regulation and supervision of service providers. A range of possible measures could be taken to ensure that the anti-money laundering requirements laid out in Recommendations 10-21 and 26-29 are observed.

(a) The means by which the authorities can determine whether there are professionals or businesses offering trust and company services to third parties as a commercial undertaking. Options include:

Option 1 - Rules or laws permitting or restricting activities being in place, and persons must declare/register that they are engaged in offering the relevant trust or company services (the

name of the entity is added to a list and the entity is allowed to carry out activities, no discretion to reject application).

Option 2 - Rules or laws permitting or restricting provision of various enumerated trust and company services, the issuance of licenses to conduct that type of business (with competent authority evaluation of the entity against criteria both initially and on an ongoing basis, and the entity is then allowed to provide the relevant services).

(b) Requirements that prevent criminals from being able to own, manage or control the service providers for illegal purposes (this is a component of (a) option 2).

Option 1 – persons with criminal records are prevented from owning, managing or controlling such a business.

Option 2 – the competent authorities have a system to ensure that they are aware whether persons with a criminal record are involved in such businesses.

Option 3 – as part of oversight the competent authorities conduct some type of fitness and properness checks on the persons engaged in these businesses.

(c) Oversight and supervision of compliance

Option 1 – Oversight by an SRO.

Option 2 – Oversight or supervision by one or more designated competent authorities (part of government). This might be either a single authority for all types of service providers and for all components of the anti-money laundering system, or different authorities could supervisor different parts of the system.

Under both options, the relevant body would need to have the appropriate powers to conduct assessments of whether a service provider is meeting its obligations.

(d) Sanctions system

The system should allow for sanctions for failing to comply with the relevant obligations. Those sanctions should be consistent, i.e. the kind of sanctions used should be similar to those applicable to financial entities. They could be criminal or administrative sanctions, or both.

5. Full regulation and supervision

As mentioned above, a number of jurisdictions seek to address not only money laundering concerns, but also issues relating to consumer/customer protection, prudential concerns, the integrity of the system as a whole etc, and consequently introduce a fuller range of measures. These additional measures, such as the duties and responsibilities of directors and trustees are mentioned above, and a further option might be to reference this broader range of measures or requirements.

5.4. Lawyers and legal professionals

272. Since the FATF first commenced studying money laundering methods and techniques on a systematic basis in 1995-96, lawyers have been consistently mentioned in FATF typologies reports as being linked to money laundering schemes and cases. A variety of reasons have been cited as to why lawyers appear to be frequently involved in money laundering:

- It has been commonly observed that criminals use lawyers client accounts for the placement and layering of funds. In many countries, this offers the advantage to the launderer of the protection that is afforded by legal professional privilege or professional secrecy.
- In a number of countries, lawyers provide a service as a "gatekeeper", that is, through their specialised expertise they are able to create the corporate vehicles, trusts, and other legal arrangements that facilitate money laundering.
- Lawyers offer the financial advice that is a required element of complex money laundering schemes.
- The use of lawyers and the corporate entities they create can provide the criminal with a veneer of respectability for the money laundering operations.

273. In addition, it has been uniformly observed both by FATF members and other international organisations that as anti-money laundering controls are effectively implemented in the financial sector, money launderers are turning to other sectors, including the use of professionals, to launder their illegal proceeds. For example, the involvement (unknowingly and otherwise) of lawyers and other professionals in money laundering cases is frequently noted in the 1998 Report of the UN Office for Drug Control and Crime Prevention on financial havens, banking secrecy and money laundering.

274. The particular role, history and status of the legal profession and the rules that attach to it, means that very careful attention will need to be given when considering the application of anti-money laundering obligations to such professionals. In particular, due to the professional secrecy or privilege that exists in relation to certain types of communications with clients, the application of the requirement to report suspicious transactions will need to be closely examined. Professional secrecy or privilege is a principle that exists in all members, but its precise boundaries vary, depending on the structure of the relevant legal system. The objective is to make it more difficult for actual or potential money launderers to attempt to misuse the services of the lawyer, while still taking into account fundamental rights.

The measures currently in place

275. Several FATF countries have already brought lawyers under the scope of their anti-money laundering regimes. New Zealand applies AML measures to lawyers engaged in certain financial activities for their clients. A number of FATF members, such as the UK, and Hong Kong, China have legislation that requires all persons to report suspicious transactions. In Canada, legal counsel are subject to AML obligations when they receive or pay funds; purchase or sell securities, real property or business assets or entities; and transfer funds or securities on behalf of any person or entity, including giving instructions in respect of those activities. However there are certain exceptions if a matter is subject to legal professional privilege.

276. Switzerland is another FATF jurisdiction where action has been taken to taken to include lawyers within the scope of their AML regime. All financial intermediaries are covered, and lawyers that provide the requisite financial services are regarded as financial intermediaries, though not with respect to the core business of a lawyer i.e. business covered by legal privilege. All intermediaries must be licensed, and are subject to customer due diligence and reporting obligations, including the obligation to report suspicious transactions to the FIU. Lawyers are also subject to supervision for anti-money laundering purposes, being supervised by an SRO, which is itself supervised by a supervisory authority.

277. The increased misuse of lawyers was noted by the European Commission and European Parliament, and led to the inclusion of lawyers under the Directive. Lawyers, who are referred to as "independent legal professionals", fall within the scope of the Directive when they are acting in the exercise of their professional activities and either:

(a) assist in the planning or execution of transactions for their client concerning the
    (i) buying and selling of real property or business entities;
    (ii) managing of client money, securities or other assets;
    (iii) opening or management of bank, savings or securities accounts;
    (iv) organisation of contributions for the creation, operation or management of companies;
    (v) creation, operation or management of trusts, companies or similar structures; or
(b) act on behalf of and for their client in any financial or real estate transaction.

278. In essence, under the Directive, independent legal professionals are brought into the fight against money laundering when they are involved in particularly vulnerable lines of business. They will be subject to know-your-customer rules and to an obligation to report suspicions of money laundering. Professional secrecy or legal professional privilege may be upheld when the lawyer is representing a client in court proceedings or is providing legal advice to ascertain the client's legal position. Thus, as stated in the preamble to the Directive, legal advice remains subject to the obligation of professional secrecy, unless the lawyer knows[42] that the client is seeking legal advice for money laundering purposes.

279. . The Directive also allows each EU Member State to legislate and provide that STR are not to be sent by lawyers (or notaries) directly to the FIU but can be sent to "an appropriate self-regulatory body of the profession". Each State will then determine how that self-regulatory body will co-operate with the competent government authorities, in particular the FIU.

280. At this time, it is proposed that the FATF framework should cover, with several options, independent legal professionals. This term is intended to cover lawyers and legal professionals that are licensed or admitted to practice and who work in law firms or are self-employed; it does not cover lawyers who have the status of employees in a legal undertaking that is not in the business of providing legal advice to third parties. A similar interpretation is taken in relation to accountants (see paragraph 294 below).

[42] In some FATF members (both within Europe and elsewhere), legal professional privilege does not apply where a lawyer suspects or strongly suspects that the client is seeking legal advice for money laundering purposes.

5.5. Notaries

5.5.1. The notarial profession

281. The profession of the notary is an ancient one and in many countries is closely linked with or is a branch of the legal profession. In almost all countries a notary or notary public (as they are referred to in some countries) is usually appointed by the government, but sometimes by the judiciary or the church. In civil law countries, a notary is a generally a public official, and the State delegates power to the notary to publicly certify and authenticate the documents that he draws up, conferring upon them probatory strength and executive force i.e. they are admissible in court without further proof of their authenticity. The notary also secures their preservation. In many jurisdictions, only "authentic acts" may be inscribed in the public records. Thus the mechanics of various registry systems, such as the registry of land ownership, often rests upon the notarial profession.

282. In order to allow independence, the notary is recognised professional status in the way the notary goes about her/his functions, which include all the activities carried out by lawyers except appearing in court. The notary has an important advisory function, ensuring compliance with the law, legal certainty and the avoidance of litigation. The notary is supposed to perform their services as an objective and neutral advisor, and can act for both parties to a transaction provided there is no conflict of interest. A notary cannot normally refuse to provide services unless the act demanded is clearly contrary to the law.

283. Notaries are required to have high educational qualifications and are subject to stringent disciplinary rules. Notaries are normally appointed for life and, except for unfitness or serious misbehaviour, cannot be removed from office. Notaries are subject to a strict obligation of professional secrecy. The nature of this obligation is slightly different from that enjoyed by other lawyers, given that notaries do not represent clients before the courts.

284. In common law countries, the functions of a notary are primarily just to witness and authenticate documents and to certify copies of those documents. However, in civil law countries or in parts of countries that apply a civil law system, notaries usually perform a much wider range of functions. The notary will typically be involved in providing legal advice, in all aspects of the conveyancing of real property, in drawing up all types of contracts, in matters of matrimonial law, inheritance law, including the drafting of wills, and the constitution and modification of companies and other commercial entities. Duties will often include advice on matters of tax law. Notaries will often handle clients' money though the situation will vary from one member to another. For example, in Japan notaries public are not supposed to keep in custody or manage their clients' money or act as gatekeepers.

5.5.2. Notaries and the fight against money laundering

285. Given the fields in which they are active, notaries are likely to encounter potential money laundering operations. In the 2000 FATF Typologies Report it was noted that:

> "62. The use of professionals specialising in the creation of legal entities as mechanisms for money laundering has already been described in the discussion of company formation agents. FATF members continued this year to note that other professions -- solicitors, notaries, and accountants, for example -- frequently play a role in money laundering schemes."

Belgium identified the creation of companies and the purchase and sale of real property as the areas in which notaries were most likely to be confronted with money laundering operations. The Netherlands reported that there had been cases in which lawyers and notaries were intentionally or unintentionally involved in suspicious transactions.

286. The notarial profession within the European Union, as well as in some other FATF members, appears to accept a role in the prevention of money laundering. A paper dated 2001 of the Conférence des Notariats de l'Union Européenne (CNUE) states (informal translation):

> "Transparency of transactions: the notary is obliged to verify the identity of the parties and participates, as a public authority and in the public interest, in the fight against money laundering and tax evasion".

5.5.3. The measures currently in place

287. At a national level, only a few FATF members currently require notaries to comply with anti-money laundering measures, e.g. Argentina, Belgium, Luxembourg, Spain, and Switzerland. For example, Argentina and Belgium require notaries to identify their customers, keep records and report suspicious transactions in a similar manner to banks and financial institutions. Switzerland also imposes anti-money laundering obligations on notaries when they are acting as financial intermediaries (see section on lawyers below for more detail).

288. The EU Directive now applies to notaries (as with other independent legal professionals) in respect of the listed types of business (financial, property and company law and fiduciary business). When legislation is enacted by each State, notaries will have to fulfil the normal client identification obligations, and will also be obliged to report suspicious transactions and implement internal control measures and train their staff concerning money laundering issues. The provisions on professional secrecy in respect of legal advice, and on the reporting obligations are the same as for lawyers (see paragraphs 277-279 above).

Options for coverage of lawyers and notaries

1. Professions to be covered

A. Lawyers

Option 1 – Lawyers and independent legal professionals in all their activities.

Option 2 – Lawyers and independent legal professionals, but only where they are acting as financial intermediaries on behalf of or for the benefit of the client.

Option 3 - Lawyers and independent legal professionals where they are involved in the planning or execution of financial, property, corporate or fiduciary business for the client.

B. Notaries

Option 1 – Notaries or notaries public, in all countries.

Option 2 – Notaries or notaries public, but only where they are acting as financial intermediaries on behalf of or for the benefit of the client.

Option 3 - Notaries or notaries public where they are involved in the planning or execution of financial, property, corporate or fiduciary business for the client.

2. Customer due diligence

Lawyers and notaries should be subject to the same customer due diligence obligations that apply to financial institutions in respect of customers activities covered in (1) above (Professions to be covered) i.e. Recommendations 10 and 11 would apply. It is also proposed that the standard set out in Recommendation 12 should apply, namely, retain records of transactions and customers for a minimum period of 5 years.

3. Suspicious transaction reporting and increased diligence

The general principle should be that lawyers and notaries would be obliged to comply with Recommendations 14-19, and in particular the reporting of suspicious transactions (though note the discussion in section 3.7.3.4. of reporting suspicious activity). However, there are several options available regarding when the reporting obligation would apply:

Option 1 - A general obligation in respect of all their activities.

Option 2 - An obligation limited to their involvement in certain listed vulnerable activities e.g. where they act as a financial intermediary.

Option 3 – apply option 1 or 2, but allow countries to decide whether STR are to be sent directly to the FIU or to the appropriate SRO (where one exists) for that profession. Each jurisdiction could determine the details of how that SRO would then co-operate with the FIU and other competent authorities.

In considering option 3 and the desirability of a level playing field, the FATF invites views on whether the SRO should have a discretion to withhold STR from the FIU.

Under all the options above, there would be no obligation to report the suspicious transaction if the relevant information came to the lawyer or notary in circumstances in which the lawyer or notary is subject to professional secrecy or legal professional privilege*. It should be noted that the rule of secrecy or privilege may not apply (depending on the laws of the country concerned) if the lawyer or notary has knowledge or a strong suspicion (in some countries, this extends to 'suspicion') that their services are being abused for money laundering or criminal purposes. Such issues or secrecy or privilege would not be relevant in countries where the notary exercises a more limited function that excludes the giving of legal advice.

Whichever option is adopted, and with one possible exception, Recommendations 14 and 16-19, which lay out other measures that are required for additional diligence should also apply. The only possible exception could be that consistent with the option provided for in the EU

Directive, Recommendation 17 would not apply to lawyers and notaries, who would be permitted to tip-off their clients that they had made a report. There are two options:

Option 1 – "Tipping-off" is permitted.
Option 2- "Tipping-off" is not permitted.

The FATF may also give further consideration as to whether it would be "tipping-off" if lawyers are required to dissuade their clients from being involved in any illegal activity.

4. Regulation and supervision

Both the legal and notarial professions are normally subject to some type of self-regulation, under which a body that represents the profession, and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory type functions. For example, it would be normal for these self-regulatory organisations (SROs) to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession. Neither lawyers nor notaries are "supervised" in the same way as financial institutions, and would not be subject to similar supervisory processes.

As there are already systems and controls governing the persons that can practice the profession, often directly or indirectly involving the State, a number of the regulatory and supervisory issues that arise concerning non-financial businesses may not be relevant to the professions. Thus, the authorities should be able to determine from such existing systems whether the persons are entitled to practice as notaries in their jurisdiction.

Similarly the State or the SRO would have in place rules and requirements that are designed to prevent or at least limit criminals from being able to own or be engaged in a legal or notarial practice, let alone run that practice for illegal purposes. It is also commonplace that there are rules and regulations that are designed to ensure that these professionals are fit and competent to practice their profession.

As regards oversight and supervision, there are several options, though some may be more practical to implement than others:

Option 1 - Self-regulatory oversight by an SRO.

Option 2 – Self-regulatory oversight by an SRO, which could itself be subject to supervision itself by a government body on compliance with AML obligations.

Option 3 – Oversight or supervision by one or more designated competent authorities (part of government).

Under both options, the relevant body would need to have the appropriate powers to conduct assessments of whether a lawyer or notary is meeting their obligations.

The system should also allow for sanctions for failing to comply with the relevant obligations. Those sanctions should be broadly proportionate and consistent with sanctions applicable to financial institutions in similar circumstances. They could be criminal, administrative or other sanctions.

* It would be for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy relating to lawyers, notaries or other professionals. This would normally cover information they receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client and (b) performing their task of defending or representing that client in, or concerning judicial proceedings, including giving advice on instituting or avoiding proceedings.

5.6. Accounting Professionals

289. As with lawyers, over recent years FATF studies of money laundering methods and techniques have linked accountants to money laundering schemes and cases, and accountants appear to be involved in money laundering for reasons similar to those applicable to lawyers:

- In a number of countries, accountants act as "gatekeepers" - through their specialised expertise they are able to create the corporate vehicles, trusts, and other legal arrangements that facilitate money laundering.
- Accountants offer financial and fiscal advice that is often a required element of complex money laundering schemes.
- The use of accountants and the corporate entities they create can provide the criminal with a veneer of respectability for their money laundering operations.
- As anti-money laundering controls are effectively implemented in the financial sector, money launderers are turning to other sectors, including the use of professionals, to launder their illegal proceeds.

290. The role that is played by external accountants[43] as "gatekeepers", whether knowingly or otherwise, and the risks that might result if they are acting for criminal clients is well established. In addition though, accountants acting as auditors also have a very important role, since they are the professionals responsible for checking financial statements, verifying the accuracy of books and records and checking on various types of controls for companies and businesses globally. Internal auditors working in financial institutions, often already have a significant role in combating money laundering and in checking the internal controls that exist within the institution. Similarly, external auditors could, in certain circumstances be well placed to perform checks on the adequacy of measures in place in the businesses in which they are conducting an audit. Other types of external accounting professionals, such as those engaged in forensic accounting or risk management could also make important contributions to combating money laundering.

291. The accounting profession has also recognised the need for members to take action concerning money laundering. In 1999, the Fédération des Experts Comptables Européens (along with other associations for accountants, lawyers, notaries and tax advisors) committed themselves to a Charter requiring national member associations to adopt codes of conduct which would help to prevent professionals being involved in organised crime. More recently, in January 2002, the International Federation of Accountants (IFAC) issued a white paper[44] that considers the role that accountants can play in efforts to prevent money laundering.

[43] The reference to "external accountants" is intended to refer to accountants exercising professional duties (including auditing functions) that practice as sole practitioners, partners or employed accountants within professional accounting firms. It is not meant to refer to 'internal' accountants that are employees of other types of businesses, nor to accountants working for government agencies, who may already be subject to measures that would combat money laundering.

[44] The paper can be located at – www.ifac.org. It lists a number of different types of accountants that may be able to play a role combating money laundering - accountants in management positions who record and report entity transactions, in-house financial systems consultants, internal auditors, practitioners who provide outsourced regulatory examination services, forensic accountants, practitioners who perform compliance and operational audits, risk management practitioners and compliance specialists, and tax practitioners.

292. Again, as with the legal profession, the particular role and history of the accounting profession, and particularly external auditors (who are often performing a statutory function) means that very careful attention will need to be given when considering the application of anti-money laundering obligations to such professionals. In particular, careful consideration will need to be given to an auditors obligations concerning the reporting of illegal activity, the rules of confidentiality or professional secrecy that apply in relation to certain types of documents or communications with clients, and the interaction with the application of the requirement to report suspicious transactions. The external auditor usually has a statutory obligation to assist the board of a company, and its shareholders, to assess if the financial statements of the company are true and correct. In some countries, this role and function means that in certain circumstances an auditor is subject to professional secrecy obligations.

The measures currently in place

293. In some FATF members, such as Switzerland, accountants that are acting as financial intermediaries are covered by the full range of anti-money laundering legislation. Similarly, in countries that have anti-money laundering legislation based on the UK model, accountants are subject to an obligation to report suspicious transactions. Belgium requires auditors and external accountants to identify their customers, keep records and, subject to certain conditions, report suspicious transactions. Canada has also applied its anti-money laundering to accountants.

294. The Directive applies to auditors and external accountants, though each jurisdiction will determine the precise scope of its anti-money laundering legislation in relation to the accounting profession. The general intention of the FATF is that at least external independent accountants and external auditors should be subject to national anti-money laundering requirements, and not persons who have accounting qualifications but have the status of employees within businesses that are not in the business of providing accounting services to third parties. Accountants that are already covered by legislative requirements that apply to them because they are employees of financial institutions (or in some countries a wider range of businesses) will not be covered by the new obligations, since this would only duplicate their existing responsibilities.

295. It should also be recalled that there already exist International Standards on Auditing (ISAs), some of which provide guidance on an auditors responsibilities concerning potentially criminal activity. For example, ISA 240 establishes standards and provide guidance on the auditor's responsibility to consider fraud and error in an audit of financial statements, while ISA 250 deals with the 'Consideration of laws and regulations in an audit of financial statements'. While not addressing the issue of money laundering, they are indicative that auditors have existing obligations when they come across potentially criminal activity in the course of their duties.

Options for coverage of accountants and auditors

In the options discussed below, in parts 1 and 4 the references to 'accountants" or 'external accountants' include auditors, while parts 2 and 3 differentiate between the obligations that could be applied to accountants and those that could apply to auditors.

1. Profession to be covered

Option 1 – All external accountants (including where the accountant is an auditor performing a statutory audit function). .

Option 2 – All external accountants, but only where they are acting as financial intermediaries). This would encompass giving advice on matters where they are acting as a financial intermediary.

2. Customer due diligence

External accountants should be subject to the same obligations as apply to financial institutions i.e. Recommendations 10 and 11 would apply. It is also proposed that the standard set out in Recommendation 12 should apply, namely, retain records of transactions and customers for a minimum period of 5 years.

External auditors may be well placed to identify money laundering, and it would seem consistent with their role and function that they should be required to undertake customer due diligence for any company or other entity that they are auditing. They should also be subject to the standard set out in Recommendation 12, namely, retain customer identification records, as well as a record of any transactions they have with the customer, for a minimum period of 5 years.

3. Suspicious transaction reporting and increased diligence

a). As with the other professions, the general principle should be that all external accountants would be obliged to comply with Recommendations 14-19, and in particular the reporting of suspicious transactions. As with lawyers, this concept might have to be extended beyond "transactions" (see section 3.7.3.4.).

b). However, there may be options as to whether or when the reporting obligation would apply to external auditors:

Option 1 - An obligation on external auditors to report suspicious transactions in respect of all their activities.

Option 2 - An obligation to report limited to their involvement in certain listed vulnerable activities e.g. where they act as a financial intermediary.

c). There are also some additional considerations applicable to all accountants (including auditors). The first is that an additional option (as for lawyers), countries could decide whether STR are to be sent directly to the FIU or to the appropriate SRO (where one exists) for that profession. Each jurisdiction could determine the details of how that SRO would then co-operate with the FIU and other competent authorities. In considering this option and the desirability of a level playing field, the FATF invites views on whether the SRO should have a discretion to withhold STR from the FIU.

Secondly, under both 3(a) and (b) above, there would be no obligation to report the suspicious transaction if the relevant information came to an external accountant or auditor in circumstances in which he was subject to professional secrecy or legal professional privilege*. Whichever option is adopted, Recommendations 14 and 16-19 (with one possible exception) should also apply if there is an obligation to report suspicious transactions. The only possible exception could be that consistent with the option provide for in the EU Directive, Recommendation 17 would not apply to accountants and auditors, who would be permitted to tip-off their clients that they had made a report. There are two options:

Option 1 – "Tipping-off" is permitted.
Option 2- "Tipping-off" is not permitted.

4. Regulation and supervision

Accountants (including auditors), like the legal professions, are normally subject to some type of self-regulation, whereby a representative body, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory type functions. Their self-regulatory organisations (SROs) apply rules to ensure that high ethical and moral standards are maintained by those practising the profession.

As regards oversight and supervision, the options that exist are thus the same as those that apply to the legal professions, and there is no obvious case for differentiating between the role of accountants generally, and that of auditors:

Option 1 - Self-regulatory oversight by an SRO.

Option 2 – Self-regulatory oversight by an SRO, which could be subject to supervision itself by a government body on compliance with anti-money laundering obligations.

Option 3 – Oversight or supervision by one or more designated competent authorities (part of government).

Under both options, the relevant body would need to have the appropriate powers to conduct assessments of whether an accountant or auditor is meeting their obligations. The same position should be adopted regarding sanctions for failing to comply with the relevant obligations.

* In certain countries accountants or auditors can be subject to professional secrecy concerning information they receive from or obtain on one of their clients when performing their task of defending or representing that client in, or assisting a lawyer concerning judicial proceedings, including giving advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

5.7. Investment advisors

296. In most countries there is a class of persons that provide financial advice or planning services to the public. These services often entail the investment advisor examining a client's financial needs and recommending financial products and services to meet those needs. In some countries, advisors that provide advice on certain types of investments; for example, pensions, life insurance, or unit trusts; must be authorised and must abide by rules to protect customers and investors. However, financial planning or advice may, depending on the country, be also offered not only by specific authorised investment advisors, but also by lawyers, accountants or other types of professionals. It may be that the advisor also offers other types of advice, such as tax planning, purchasing foreign real estate etc.

297. The proposal in section 3.1 for defining a financial institution covers a wide variety of financial activities, including providing various investment services for a client, whereby the financial institution handles and invests the client's money or funds. This could extend to the provision of investment advice, where this is linked to the advisor handling client funds. However, it does not currently include advisors or entities that only provide advice and which do not themselves handle the client's funds. Given that investment advisors occupy an important role as financial intermediaries, and are often particularly well placed to know the client's affairs, consideration should be given as to whether they should be subject to AML obligations, even where they do not handle the client's funds.

The measures currently in place

298. Several FATF countries have already brought investment advisors under the scope of their anti-money laundering regimes, and some treat financial advisors in a similar way to financial institutions. The United Kingdom applies AML measures to independent financial advisors, who are also a regulated financial institution. Similarly, Belgium regulates investment companies, investment intermediaries and advisors in the form of a financial management company. In the Netherlands, tax advisors[45] will soon be subject to reporting obligations. In those countries, the investment intermediaries and advisors have played a role in the fight against money laundering, and made a significant number of STR.

Options for coverage of investment advisors

1. Business or profession to be covered by AML obligations

All businesses or persons that, as a commercial undertaking, provide advisory services to third parties relating to the investment of funds or monies by the third party, should be subject to AML obligations.

Where particular classes of professionals, in particular lawyers or accountants, are subject to some or all of the FATF Recommendations in respect of all or part of the investment advice activity they undertake, there will be a need to ensure that the obligations imposed are consistent.

[45] See also changes concerning tax advisors in the amended EU Directive.

2. Customer due diligence

Investment advisors should be subject to the same customer due diligence as apply to financial institutions i.e. Recommendations 10 and 11 would apply. It is also proposed that the standard set out in Recommendation 12 should apply, namely, retain records of transactions and customers for a minimum period of 5 years.

3. Suspicious transaction reporting and increased diligence

The general principle should be that investment advisors would be obliged to comply with Recommendations 14-19, and in particular the reporting of suspicious transactions, although this concept would have to be extended beyond "transactions" to capture the giving of advice or similar activity (see section 3.7.3.4.). If the investment advisor is a lawyer, notary, accountant or auditor then the obligation to report the suspicious transaction may depend on any applicable professional secrecy or legal professional privilege (see section 5.4.).

4. Anti-money laundering regulation and supervision

As the provision of investment advice is performed by several different types of professions or businesses, and the legislative action that has been taken at a national level varies widely, there is no uniform position concerning the regulation and supervision of such advisors. A range of possible measures could be taken to ensure that the anti-money laundering requirements laid out in Recommendations 10-21 and 26-29 are observed.

(a) The means by which the authorities can determine whether there are professionals or businesses offering investment advisory services to third parties as a commercial undertaking.

Options include:

Option 1 - Rules or laws permitting or restricting activities being in place, and persons must declare/register that they are engaged in offering the relevant investment advisory services (the name of the entity is added to a list and the entity is allowed to carry out these activities, no discretion to reject application).

Option 2 - Rules or laws permitting or restricting provision of various enumerated investment advisory services, the issuance of licenses to conduct that type of business (with competent authority evaluation of the entity against criteria both initially and on an ongoing basis, and the entity is then allowed to provide the relevant services).

(b) Requirements that prevent criminals from being able to own, manage or control investment advisors for illegal purposes (this is a component of (a) option 2).

Option 1 – persons with criminal records are prevented from owning, managing or controlling such a business.

Option 2 – as part of oversight the competent authorities conduct some type of fitness and properness checks on the persons engaged in these businesses.

(c) Oversight and supervision of compliance

Option 1 – Oversight by an SRO.

Option 2 – Self-regulatory oversight by an SRO, which could be subject to supervision itself by a government body on compliance with anti-money laundering obligations.

Option 3 – Oversight or supervision by one or more designated competent authorities (part of government). This might be either a single authority for all types of investment advisors and for all components of the AML system, or different authorities could supervise different parts of the system.

Under both options, the relevant body would need to have the appropriate powers to conduct assessments of whether an investment advisor is meeting its obligations.

(d) Sanctions system

The system should allow for sanctions for failing to comply with the relevant obligations. Those sanctions should be consistent, i.e. the kind of sanctions used should be similar to those applicable to financial entities. They could be criminal or administrative sanctions, or both.

5. Full regulation and supervision

As mentioned above, a number of jurisdictions seek to address not only money laundering concerns, but also issues relating to customer and investor protection, prudential concerns, the integrity of the system as a whole etc, and consequently introduce a fuller range of measures. These additional measures, which may be similar to the controls that apply to financial institutions, provide a further option.

GLOSSARY

In the consultation paper the following abbreviations and references are used:

"**AML**" = anti-money laundering

"**the Annex**" refers to the Annex to Recommendation 9 of the Forty Recommendations.

"**Banks**" means financial sector entities that are covered by the BIS core principles for banking supervision.

"**Basel CDD paper**" refers to the guidance paper on Customer Due Diligence for Banks issued by the Basel Committee on Banking Supervision in October 2001.

"**Beneficial ownership**" refers to the natural person(s) who ultimately own(s) or control(s) a customer or their assets, and/or the person on whose behalf a transaction is being conducted. This incorporates the concepts contained in the definition of "beneficial ownership" for corporate vehicles set out in paragraph 20 of "the OECD report", namely –

> "In this Report, *"beneficial ownership"* refers to ultimate beneficial ownership or interest by a natural person. With respect to corporations, ownership is held by shareholders[46] or members. In partnerships, interests are held by general and limited partners. In trusts and foundations, beneficial ownership refers to beneficiaries, which may also include the settlor or founder."
>
> It also incorporates those persons who exercise ultimate effective control over a 'corporate vehicle.

"**Corporate Vehicles**" covers the following entities referred to in "the OECD report":

- Corporations – (a) private limited companies and public limited companies whose shares are not traded on a stock exchange, (b) international business companies/exempt companies.
- Trusts
- Foundations.
- Limited partnerships and limited liability partnerships.

"**Competent authorities**" refers to those agencies of government that carry out supervisory or regulatory responsibility for financial institutions and other entities (where appropriate).

"**Entity**" could refer to natural or legal persons.

"**EU Directive**" refers to EU Directive 91/308/EEC, as amended by the second EU anti-money laundering Directive adopted on 4 December 2001.

"**FATF 40**" means the FATF Forty Recommendations and Interpretative Notes.

[46] Ownership and control of a company may also be influenced by other methods of holding an interest in a company, other than shares e.g. options or warrants.

"**FATF framework**" = the FATF 40, the Terrorist Financing Recommendations and the NCCT Criteria.

"**Financial institutions**" = means the entities that carry out the activities set out in Section 3.1 – effectively banks and non-bank financial institutions.

"**FIU**"= Financial Intelligence Unit

"**NCCT**" = Non-Cooperative Countries or Territories

"**NCCT Criteria**" = refers to the 25 Criteria published in the FATF Report on NCCT issued in February 2000.

"**Non-bank financial institutions or NBFIs**" = financial institutions that are not banks.

"**Non-financial businesses or professions**" = entities other than financial institutions and whose role in combating money laundering is dealt with in Section 5 of this paper.

"**OECD Report**" means the OECD Report entitled "Behind the Corporate Veil - Using Corporate Vehicles for Illicit Purposes" issued in 2001.

"**PEP**" means Politically Exposed Person.

"STR" = suspicious transaction report.

ANNEXES TO THE CONSULTATION PAPER ON THE REVIEW OF THE FATF FORTY RECOMMENDATIONS

ANNEX 1

Possible Measures for Managing Money Laundering Risks in Non-Face-To-Face Customer Relationships

Establishing customer relationships

1. In accepting business from non-face-to-face customers, institutions should apply equally effective customer identification procedures for non-face-to-face customers as for face-to-face customers; and there must be specific and adequate measures to mitigate any higher risk.

2. Maintain the requirement of face-to-face verification for all new customers to ascertain their identity, including:
   - by the branches of the institution; or
   - by relying on third parties (in accordance with the requirements set out in section 5.5).

3. Require face-to-face verification for any new customers who fall into certain categories, e.g., those with assets exceeding a specified sum, or who reside in jurisdictions that are renowned money laundering risks or where identify fraud is common.

4. Provide sophisticated online questionnaires for account opening applications. Such questionnaires could give the institution a higher comfort level that the person is who they say they are because they could provide a wide range of information capable of verification from other sources. Moreover, a sophisticated online questionnaires for account opening applications that obtains information about the activities, the major clients and the income of the client enhances the ability of the institution to conduct ongoing due diligence of the customer relationship and is not necessarily more difficult than where there is face-to-face contact. Moreover, capturing the information electronically may enhance the [service provider's/institution's] ability to identify suspicious or unusual activity during the relationship through using monitoring technology.

5. Carry out electronic checks across several databases, or of one single database that bring together information from a variety of different sources, to corroborate the information provided by the applicant (e.g. that a person of the applicant's name is recorded at the address given by them etc).

6. To send a letter by registered post to validate the address of the client. (Some financial institutions send customers by way of a registered letter payment instruments or codes. The account is not activated until the signed acknowledgement of receipt is returned).

7. To request another original document to verify the address of the customer concerned – e.g. their latest telephone, gas and electricity bill.

8. To make a "physical" validation, for example, an initial telephone call by institution staff to a telephone number that has been independently checked with the institution.

9. Requiring the first payment to be carried out through an account in the customer's name with another institution that is subject to FATF customer due diligence standards.

10. Using certificates issued under electronic signature procedures – although the level of comfort provided could vary depending on the methods used by the [service provider that authenticated the electronic signature.

11. Use biometrics and other emerging technologies to validate the customer's true identity.

12. Not allowing customers to establish relationships without face-to-face contact if the financial institution suspects or has reason to believe that the customer is avoiding face-to-face contact in order to hide his or her true identity and/or money laundering is involved.

13. Requiring the financial institution's auditors to periodically review account opening procedures for non-face-to-face business.

Ongoing due diligence

14. When the customer has been identified, any contact and conduct of transactions should be via a secure password access system to help assure the financial institution that it is dealing with the customer and not someone who has assumed the customer's identity.

15. Technology can be used to keep on-going due diligence information up to date, since it may be easier to ask customers questions more regularly, and update customer profiles than when using manual systems. System triggers can be built into the product/service offering to validate transactions in light of existing customer information.

16. To require face-to-face verification for certain types of transaction.

17. Establishing transaction limits for automated processing.

18. Require institutions to establish computerised monitoring systems to assist in their scrutiny of customer activity and search for unusual activity. However, any systems should be tools only - not the sole method for scrutinising customer activity. institution staff still need monitor transactions carried out on an account and be familiar with the pattern of activity on an account.

19. The financial institutions could use technology to require additional validation procedures for certain customers or transactions (e.g. when transactions fall outside of usual patterns). These could include:
    - Additional questions about the nature of the transaction.
    - A process that requires the transaction to be manually authorised by a staff member of the institution.

20. Institutions should monitor deposits and withdrawals through an account when these occur at different physical locations, particularly in different jurisdictions and especially

if the geographical spread/distance is difficult for the customer to physically cover in the time period that the transactions are carried out over.

Electronic money/ purses/cards

21. Impose limits on any single transaction.

22. Forbid or restrict customer-to-customer transactions.

23. Take particular care to scrutinise:
    - excessive requests for e-money or repeated requests for the reimbursement of the unspent value of e-money by individual distributors;
    - anomalous sales volumes with respect to an individual merchant's type of activity;
    - frequent or large (even if split up) requests by customers for the reimbursement of amounts concerning unused e-money credits.

24. Restrict issuance to financial institutions that are required to comply with FATF standards.

25. Link purses/cards to a dedicated account with a institution so that the amount of money that can be spent is the value stored in the account, not on the purse/card itself.

26. Only allow reloading above certain amounts through debiting an account held with a financial institution that is subject to customer due diligence requirements.

27. Only allow the purses/cards to be debited to pay merchants where purchases are made.

28. Do not allow bearer purses/cards to be recharged.

29. Restrict merchants to those who are approved by a competent authority or by the financial institution that issues the purses/cards after it has carried out due diligence on the merchant.

30. Require the purse/card or the system it operates on to record all transactions or all transactions over certain amounts so that traceable records are available to investigative agencies if needed.

ANNEX 2

Simplified Customer Identification/Verification obligations for financial institutions

This describes the situation where a financial institution or another type of company from another country seeks to establish a business relationship or account at a financial institution in an FATF member country. The second column sets out whether such credit institution (CI) or financial institution (FI) customers (from the other country) are subject to simplified or reduced identification/verification requirements, and the last column shows with respect to which jurisdictions this applies.

Member	Institutions	Jurisdictions
Austria	CI	EEA (EU, Norway, Iceland and Liechtenstein)
Belgium	CI or FI covered by the EU Directive 91/308/EEC	EEA
Canada	1.Corporations with net assets greater than CAD 75 million that are publicly listed on a Canadian or a prescribed foreign stock exchange from an FATF country. 2.Regulated Canadian pension funds	Any if listed as required
Denmark	CI or FI covered by the EU Directive 91/308/EEC	EEA
Finland	Credit institutions, financial institutions, investment firms and life insurance companies and their branches authorized in EEA	EEA
Germany	CI or FI covered by the EU Directive 91/308/EEC	If equivalent supervision to CI
Greece	CI or FI covered by the EU Directive 91/308/EEC	FATF
Iceland	CI or FI licensed to provide the services in Annex to Recc. 9	EEA
Ireland	CI & FI corresponding to institutions covered by Irish anti-money laundering legislation	FATF, Jersey, Guernsey and Isle of Man.
Italy	Any FI which is: (1) an authorised intermediary, (2) previously identified by the FIU, (3) operating on its own behalf	Any
Luxembourg	CI & FI	FATF & EEA
Mexico	FI	All
Netherlands	CI, insurance companies (IC) and investment firms (IF), and investment services (IS) registered at an Exchange in an FATF member	EU (CI, IC, IF) FATF (IS)
New Zealand	No general exemption, except where FI conducts transaction on behalf of a client (and that FI has an obligation to identify its client)	Applies to NZ FIs only
Portugal	CI, life insurance companies and investment firms, & branches of non-EEA institutions located in EEA	EEA

Spain	CI & FI acting as clients on its own behalf	EEA
Sweden	CI & FI, if subject to anti-ML laws	EEA
Switzerland	No general exemption, except CI & FI can renounce the need to identify publicly known client e.g. listed company	Countries with anti-ML systems at least equivalent to Swiss & FATF systems
Turkey	CI & State enterprises	
U.K.	CI & FI	FATF, Gibraltar, Jersey, Guernsey and the Isle of Man (JMLSG), EEA & countries with anti-ML systems (FSA)

9 Members with no "exemptions"
Argentina, Australia, Brazil, France; HK, China; Japan, Norway, Singapore, U.S.

ANNEX 3

Reliance on third parties to perform certain Customer Identification/Verification functions

In many countries a financial institution or other businesses or persons subject to customer identification functions are entitled to rely on other institutions or persons (other than their own staff) to identify and/or verify the identity of their customers.

- The first column shows the types of institutions or persons that can rely on a third party to perform these functions.
- The second column sets out the types of third parties that can perform the functions.
- The last column shows the jurisdictions from which the third party can come.

Member	Institution relying on a third party	Type of third party	Jurisdiction of third party
Australia	All institutions or businesses s.t. obligation	1. List of "acceptable referees" 2. Foreign bank employee	1. Australia 2. Any
Austria	Banks	Lawyers or notaries in limited circumstances	Austria
Canada	1.Internet Bank or other FI 2. Securities dealer	1. Canadian deposit taking institution where it holds an account 2. Foreign securities dealer (s.t. conditions)	Canada Foreign country (FATF and others with equivalent standards)
Finland	All institutions or businesses s.t. obligation	Other institutions s.t. anti-ML obligations, or post office	
Germany	CI/FI	Trustworthy 3rd parties e.g. banks, FI, notaries, post offices, embassies, other	Primarily EU, but could be wider
Hong Kong, China	Banks	1. Banks, securities and insurance if regulated, or 2. Other intermediary - if primary institution is satisfied and has relationship with it	1. FATF 2. Any
	Securities and futures firms	Regulated firms, professionals e.g. bank manager, notary public, lawyers, post office	Any
	Insurance companies	Insurance agents and brokers (s.t. anti-ML guidelines)	Any
Italy	Authorised intermediaries	Banks	Foreign country (FATF and others with equivalent standards)

Netherlands	Insurance company	Insurance broker	
New Zealand	FI	Other FI (if operating in NZ)	NZ
Singapore	Banks, finance companies, securities and futures firms (for non-Singapore residents)	Branches or subsidiaries of bank, correspondent bank or lawyers/notaries public	Any
Switzerland	1. Banks 2. Other financial intermediaries	1. Any person mandated 2. Other FI having relationship with customer	
U.K.	FI	Regulated entity	Countries with anti-ML systems equivalent to EU Directive
Belgium, Brazil, Greece, Japan, Portugal, Spain	No reliance on third parties permitted		

ANNEX 4

Extracts from the FATF 40, the Terrorist Financing Recommendations and the NCCT Criteria

FATF 40

Recommendation 8

Recommendations 10 to 29 should apply not only to **banks**, but also to **non-bank financial institutions**. Even for those non-bank financial institutions which **are not subject to a formal prudential supervisory regime** in all countries, for example bureaux de change, governments should ensure that these institutions are **subject to the same anti-money laundering laws or regulations** as all other financial institutions and that these laws or regulations are **implemented effectively**.

Interpretative Note to Recommendation 8

The FATF Recommendations should be applied in particular to **life insurance and other investment products offered by insurance companies**, whereas Recommendation 29 applies to the whole of the insurance sector.

Recommendation 9

The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a **commercial undertaking by businesses or professions** which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to **each country to decide** whether special situations should be defined where the application of **anti-money laundering measures** is **not necessary**, for example, when a financial activity is carried out on an **occasional or limited basis**.

Interpretative Note to Recommendations 8 and 9 (Bureaux de Change)

Introduction

Bureaux de change are an important link in the money laundering chain since it is difficult to trace the origin of the money once it has been exchanged. Typologies exercises conducted by the FATF have indicated increasing use of bureaux de change in laundering operations. Hence it is important that there should be effective counter-measures in this area. This Interpretative Note clarifies the application of FATF Recommendations concerning the financial sector in relation to bureaux de change and, where appropriate, sets out options for their implementation.

Definition of Bureaux de Change

For the purpose of this Note, bureaux de change are defined as institutions which carry out retail foreign exchange operations (in cash, by cheque or credit card). Money changing operations which are conducted only as an ancillary to the main activity of a business have already been covered in Recommendation 9. Such operations are therefore excluded from the scope of this Note.

Necessary Counter-Measures Applicable to Bureaux de Change
To counter the use of bureaux de change for money laundering purposes, the relevant authorities should take measures to **know the existence of all** natural and legal persons **who, in a professional capacity, perform foreign exchange transactions**.

As a **minimum requirement**, FATF members should have an effective system whereby the bureaux de change are known or declared to the relevant authorities (whether regulatory or law enforcement). One method by which this could be achieved would be a requirement on bureaux de change to submit to a designated authority, a simple declaration containing adequate information on the institution itself and its management. The authority could either issue a receipt or give a tacit authorisation: failure to voice an objection being considered as approval.

FATF members could also consider the introduction of a formal authorisation procedure. Those wishing to establish bureaux de change would have to submit an application to a designated authority empowered to grant authorisation on a case-by-case basis. The request for authorisation would need to contain such information as laid down by the authorities but should at least provide details of the applicant institution and its management. Authorisation would be granted, subject to the bureau de change meeting the specified conditions relating to its management and the shareholders, including the application of a "fit and proper test".

Another option which could be considered would be a combination of declaration and authorisation procedures. Bureaux de change would have to notify their existence to a designated authority but would not need to be authorised before they could start business. It would be open to the authority to apply a 'fit and proper' test to the management of bureaux de change after the bureau had commenced its activity, and to prohibit the bureau de change from continuing its business, if appropriate.

Where bureaux are required to submit a declaration of activity or an application for registration, the designated authority (which could be either a public body or a self-regulatory organisation) could be empowered to publish the list of registered bureaux de change. As a minimum, it should maintain a (computerised) file of bureaux de change. There should also be powers to take action against bureaux de change conducting business without having made a declaration of activity or having been registered.
As envisaged under FATF Recommendations 8 and 9, **bureaux de change should be subject to the same anti-money laundering regulations as any other financial institution**. The FATF Recommendations on financial matters should therefore be applied to bureaux de change. Of **particular importance** are those on **identification requirements, suspicious transactions reporting, due diligence and record keeping**.

To ensure effective implementation of anti-money laundering requirements by bureaux de change, **compliance monitoring mechanisms should be established and maintained**. Where there is a registration authority for bureaux de change or a body which receives declarations of activity by bureaux de change, it could carry out this function. But the **monitoring** could also be done **by other designated authorities (whether directly or through the agency of third parties such as private audit firms)**. Appropriate steps would need to be taken against bureaux de change which failed to comply with the anti-laundering requirements.

The bureaux de change sector tends to be an unstructured one without (unlike banks) national representative bodies which can act as a channel of communication with the authorities. Hence it is important that FATF members should establish effective means to ensure that bureaux de change are aware of their anti-money laundering responsibilities and to relay information, such as guidelines on suspicious transactions, to the profession. In this respect it would be useful to encourage the development of professional associations.

Recommendation 26

The **competent authorities** supervising banks or other financial institutions or intermediaries, or other competent authorities, **should ensure** that the **supervised institutions** have adequate programs to guard against money laundering. These authorities should co-operate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

Recommendation 27

Competent authorities should be **designated** to ensure an **effective implementation** of all these Recommendations, through **administrative supervision and regulation**, in other professions dealing with cash as defined by each country.

Recommendation 28

The **competent authorities should establish guidelines** which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

Recommendation 29

The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against **control or acquisition of a significant participation in financial institutions by criminals or their confederates**.

Interpretative Note to Recommendation 29

Recommendation 29 should **not be read as to require** the introduction of a system of regular review of licensing of controlling interests in financial institutions **merely for anti-money laundering purposes**, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or "fit and proper") tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Terrorist Financing Recommendations

Recommendation VI. Alternative Remittance

Each country should take measures to ensure that persons or legal entities, including agents, that **provide a service for the transmission of money or value, including** transmission

through an **informal money or value transfer system** or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

NCCT Criteria

NCCT 1. Absence or ineffective regulations and supervision for all financial institutions in a given country or territory, onshore or offshore, on an equivalent basis with respect to international standards applicable to money laundering.

NCCT 2. Possibility for individuals or legal entities to operate a financial institution without authorisation or registration or with very rudimentary requirements for authorisation or registration.

NCCT 3. Absence of measures to guard against holding of management functions and control or acquisition of a significant investment in financial institutions by criminals or their confederates.

ANNEX 5

TYPES OF TRUSTS

1. In legal terms, a trust exists where a person (known as a trustee) holds or has vested in him or is deemed to hold or have vested in him property, of which he is not the owner in his own right, for:

(a) the benefit of any person (known as a beneficiary) whether or not yet ascertained or in existence; or
(b) any purpose; or
(c) for the benefit of (a) and (b) above.

2. What this means is that a "trust" is a legally binding arrangement where one person (a "trustee") owns assets not for his own use and benefit, but for the benefit of others (the "beneficiaries"). It is normal, but not essential, for a trust to be constituted in writing in the form of a "trust deed" or "trust instrument" which will set out the manner in which the beneficiaries can benefit from the trust, as well as the powers and duties which the trustees will have in administering the trust and its assets. The person transferring assets to the trustee is known as the "settlor". The settlor may also in some cases be a beneficiary.

3. In all jurisdictions where the law makes provision for trusts on Anglo-American lines, trusts involve trustees, beneficiaries and settlors. The Hague Convention on the Law Applicable to Trusts and on their Recognition defines a trust as "the legal relationship created, inter vivos or in death, by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or a specified purpose."

- **Trustees;** the trustees, who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a *protector*, who may have power to veto the trustees' proposals or remove them, and/or a *custodian* trustee, who holds the assets to the order of the managing trustees.

- **Beneficiaries;** all trusts (other than charitable or statutory permitted non-charitable trusts) must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.

- **Settlors;** the settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. In the case of discretionary trusts, where the

trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

4. There are many reasons why an individual may wish to set up a trust - which means handing over the legal ownership and the control of the assets to another person - the trustee. These include:

- to allow more than one generation to enjoy the use of a property;
- to provide for incapacitated persons;
- to protect family property from spendthrifts;
- to enable the centralisation and co-ordination of world-wide assets;
- to avoid forced heirship provisions;
- as part of a tax planning strategy;
- to provide pensions for retired employees and their dependants;
- to facilitate investments through unit trusts;
- as part of a corporate financing structure;
- to raise funds for charities.

Types of Trusts

5. Of the most common forms of "express trusts", whereby the settlor has established the trust through a written trust deed, one can distinguish between those for private benefit on the one hand and those for public benefit on the other.

6. Private Trusts

(i) Discretionary Trust

This is a form of trust where the interests of the beneficiaries are not fixed but depend upon the exercise by the trustee of some discretionary powers in their favour. As such it is the most flexible of all trusts and the most common form of trust used.

(ii) Interest in Possession Trust

This is a trust where a particular beneficiary (the "life tenant") has a right to receive all the income arising from the trust fund during his lifetime. The trustee will usually also have a power to apply capital to the life tenant. Often there are successive life interests in favour of an individual and his spouse. On the death of the life tenant the trust fund is typically held on discretionary trusts for a named class of beneficiaries.

(iii) Fixed Trust

A trust where the interests of beneficiaries are fixed. The trustees will have control over the management of the assets but could not vary the amount paid to the beneficiary, or any other interest the beneficiary may have in the assets in the trust. Traditionally the trusts provide an income which is paid to the wife and capital to the children on her death.

(iv) Accumulation and Maintenance Trust

This form of trust is usually created for the children or grandchildren of the settlor, where the trustees have powers during the minority of each beneficiary to pay income in a way beneficial to the upbringing or education of the beneficiary, and to accumulate income not so applied. On attaining a certain age each beneficiary will become entitled to a particular share of the trust fund.

(v) Protective Trust

A trust where the interest of a beneficiary will be reduced or terminated if the beneficiary attempts to alienate or dispose of his interest in income or capital. Essentially, this form of trust protects the beneficiary from the temptation to sign away his or her rights to the assets in the trust.

(vi) Asset Protection Trust

A trust established with a view to protecting trust assets from a future bankruptcy or legal liability of the settlor. (Some offshore centres have introduced legislation to permit asset protection trusts; others have no such legislation and their Courts would be expected to set aside trusts designed to prejudice foreseen creditors.)

(vii) Employee Share/Options Trusts

Trusts established by institutions in favour of employees. Benefits can be deferred.

(viii) Purpose Trusts

A trust established for one specific purpose or transaction. May be established where it is desirable to isolate the purpose or transaction from the other activities or a party involved in the transaction. There are no named or ascertainable beneficiaries but there must be an enforcer to enforce the terms of the purpose trust.

(ix) Settlor Directed Trusts

A trust established with provisions enabling the settlor to direct the trustees in investment matters and/or asset distributions.

7. Public Trusts

(i) Charitable Trusts

A trust established purely for charitable purposes. In this case, there needs to be an enforcer, who can enforce the trust for the benefit of the charitable purposes. Such trusts are of unlimited duration.

(ii) Commercial Trusts

The major applications include:-

- pension fund trusts
- unit trusts
- debenture trusts for bond holders
- securitisation trusts for balance sheet reconstructions
- client account trusts for lawyers and other providers of professional services, separate from the provider's own assets

- retention fund trusts, pending completion of contracted work

8. Other Trusts

The trusts described above are essentially forms of "express trust"., where the settlor has established the trust in the form of a trust deed. However, a trust can also arise from an oral declaration or by conduct and may be deemed to have been created by the court in certain circumstances.

(i) Implied trusts

Implied trusts may be express trusts where the intention of the settlor or testator is implied in the non-technical language which he has used or where the trust arises by operation of law, as in the case of constructive and resulting trusts. On account of their very nature, there are no formality requirements for those trusts which arise by operation by law. Usually the existence of such trusts is only recognised as a result of legal action and the terms are invariably set out in a court order.

(ii) Constructive trusts

Constructive trusts are those trusts which are constructed, as it were, on the basis of the presumed intention of the settlor or testator or, irrespective of intention, imposed by a court of equity in circumstances in which it would be unconscionable or inequitable for a person holding property to keep it for his own use and benefit absolutely. In a recent case, a judge subdivided constructive trusts into two distinct categories – "distinguishing the constructive trust proper, where equity intervenes to prevent the legal owner from unconscionably denying the beneficial interest of another, from the so-called constructive trust, where equity intervenes to provide relief against fraud by making those implicated in the fraud accountable as if they were trustees.

(iii) Resulting trusts

Resulting trusts are trusts which occur either where a rebuttable presumption of intention has arisen that property held by one person is owned beneficially by another, such as where A provides the purchase money for a house that is vested in B's name, or where a person transfers property to another on trusts which initially or subsequently fail to dispose wholly of his beneficial interest so that the extent of his indisposed interest, it is said, results to that person. An example of this latter type is where ultimate default trusts are omitted from a settlement deed or where a contingent interest fails to vest indefeasibly and absolutely in the beneficiaries under that settlement.

9. Conclusion

This description of trusts show that the concept encompasses a wide variety of arrangements. Essential to them all is that the legal ownership and control is passed from the settlor to the trustee. In some cases, the settlor may attempt to gain the advantages of foregoing the legal ownership of assets, while still retaining full

effective control. The courts have established that, in such cases, depending on the circumstances, the trust can be set aside as a sham, on the basis that trust ownership and control have not in fact passed from the settlor to the trustee.