Supplement to the Study Guide for the CAMS Certification Examination

Fourth Edition

A Publication of the

Association of Certified Anti-Money Laundering Specialists®

ACAMS®

Executive Director
Gregory Calpakis, CAMS

Editor
Saskia Rietbroek-Garcés, CAMS

Contributors
Mary Bhawnani
John Byrne, CAMS
Garry Clement, CAMS
Michael R. McDonald, CAMS
Christopher Myers, CAMS
Eugene M. Propper
John Pyrik, CAMS
Nancy Saur, CAMS
Jeffrey Sklar, CAMS

Published By
Association of Certified Anti-Money
Laundering Specialists (ACAMS)
Brickell Bayview Center
80 Southwest 8th Street
Suite 2350
Miami, FL 33130 United States
ACAMS.org
ACAMS.org/espanol

Tel: +1.305.373.0020
Fax: +1.305.373.5229
Fax: +1.305.373.7788
ACAMS.org
ACAMS.org/espanol
E-mail: info@ACAMS.org

 ISBN: 978-0-9777495-3-9

For your convenience, the *Supplement to the Study Guide for the CAMS Certification Examination* includes reference materials that will help you prepare for and enhance your performance on the Certified Anti-Money Laundering Specialist® (CAMS) examination.

While the enclosed reference documents are crucial to a candidate's successful completion of the CAMS certification examination, we encourage you to review the other references cited in chapter nine, "Guidance Documents and Reference Materials", of the *Study Guide for the CAMS Certification Examination*. Although the *Supplement to the Study Guide* includes a select set of reference documents that are relevant to the CAMS certification examination, the *Study Guide* includes detailed information on how to access the additional resources.

Good luck!

Association of Certified Anti-Money Laundering Specialists

TABLE OF CONTENTS

Financial Action Task Force on Money Laundering — The Forty Recommendations and Interpretative Notes

Financial Action Task Force on Money Laundering
June 20, 2003 (Incorporating the Amendments of October 22, 2004)

Introduction

Money laundering methods and techniques change in response to developing counter-measures. In recent years, the Financial Action Task Force (FATF)[1] has noted increasingly sophisticated combinations of techniques, such as the increased use of legal persons to disguise the true ownership and control of illegal proceeds, and an increased use of professionals to provide advice and assistance in laundering criminal funds. These factors, combined with the experience gained through the FATF's Non-Cooperative Countries and Territories process, and a number of national and international initiatives, led the FATF to review and revise the Forty Recommendations into a new comprehensive framework for combating money laundering and terrorist financing. The FATF now calls upon all countries

1 *The FATF is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing. It currently has 33 members: 31 countries and governments and two international organisations; and more than 20 observers: five FATF-style regional bodies and more than 15 other international organisations or bodies. A list of all members and observers can be found on the FATF website at http://www.fatf-gafi.org/Members_en.htm.*

to take the necessary steps to bring their national systems for combating money laundering and terrorist financing into compliance with the new FATF Recommendations, and to effectively implement these measures.

The review process for revising the Forty Recommendations was an extensive one, open to FATF members, non-members, observers, financial and other affected sectors and interested parties. This consultation process provided a wide range of input, all of which was considered in the review process.

The revised Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing. The FATF recognises that countries have diverse legal and financial systems and so all cannot take identical measures to achieve the common objective, especially over matters of detail. The Recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks. The Recommendations cover all the measures that national systems should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and certain other businesses and professions; and international co-operation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering typologies. The 1996 Forty Recommendations have been endorsed by more than 130 countries and are the international anti-money laundering standard.

In October 2001 the FATF expanded its mandate to deal with the issue of the financing of terrorism, and took the important step of creating the 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.[2]

---

2 *The FATF Forty and Eight Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and the financing of terrorism.*

A key element in the fight against money laundering and the financing of terrorism is the need for countries systems to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and FATF-style regional bodies, as well as the assessments conducted by the IMF and World Bank, are a vital mechanism for ensuring that the FATF Recommendations are effectively implemented by all countries.

THE FORTY RECOMMENDATIONS

A. LEGAL SYSTEMS

Scope of the Criminal Offence of Money Laundering

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

   Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

   Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences.[3]

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

2. Countries should ensure that:

    a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

    b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisonal Measures and Confiscation

3. Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences,

3 See the definition of "designated categories of offences" in the Glossary.

instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

Customer Due Diligence and Record-Keeping

4. Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

5.* Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- Establishing business relations;
- Carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative

* *Recommendations marked with an asterisk should be read in conjunction with their Interpretative Note.*

Note to Special Recommendation VII;

- There is a suspicion of money laundering or terrorist financing; or
- The financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.[4]

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that 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, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or

4 Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

6.* Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.

b) Obtain senior management approval for establishing business relationships with such customers.

c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced ongoing monitoring of the business relationship.

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering

or terrorist financing investigation or regulatory action.

b) Assess the respondent institution's anti-money laundering and terrorist financing controls.

c) Obtain approval from senior management before establishing new correspondent relationships.

d) Document the respective responsibilities of each institution.

e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

8. Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with nonface to face business relationships or transactions.

9.* Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from

the third party upon request without delay.

b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

10.* Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

11.* Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

12.* The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-

financial businesses and professions in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of Suspicious Transactions and Compliance

13.* If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law

or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

14.* Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

15.* Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

b) An ongoing employee training programme.

c) An audit function to test the system.

16.* The requirements set out in Recommendations 13 to 15, and 21 apply to all designated nonfinancial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones

should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Other Measures to Deter Money Laundering and Terrorist Financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

19. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

20. Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures To Be Taken With Respect to Countries That Do Not or Insufficiently Comply With The FATF Recommendations

21. Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

22. Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and Supervision

23.* Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory

and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

24. Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

    a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:

        - Casinos should be licensed;
        - Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino
        - Competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

    b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-

regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

25.* The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.

C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent Authorities, Their Powers and Resources

26.* Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

27.* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries.

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in

prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.

31. Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of Legal Persons and Arrangements

33. Countries should take measures to prevent the unlawful use of legal

persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

34. Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

International Co-Operation

35. Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Mutual Legal Assistance and Extradition

36. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.

b) Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.

c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

37. Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

38.* There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure

and confiscation proceedings, which may include the sharing of confiscated assets.

39. Countries should recognise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

    Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other Forms of Co-Operation

40.* Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

    a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

    b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

    c) Competent authorities should be able to conduct inquiries;

and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that

information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

GLOSSARY

In these Recommendations the following abbreviations and references are used:

"Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

"Core Principles" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

"Designated categories of offences" means:

- Participation in an organised criminal group and racketeering;
- Terrorism, including terrorist financing;
- Trafficking in human beings and migrant smuggling;
- Sexual exploitation, including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint and hostage-taking;

- Robbery or theft;
- Smuggling;
- Extortion;
- Forgery;
- Piracy; and
- Insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

"Designated non-financial businesses and professions" means:

a) Casinos (which also includes internet casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

   - Acting as a formation agent of legal persons;
   - Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
   - Providing a registered office; business address or accommodation, correspondence or administrative address

for a company, a partnership or any other legal person or arrangement;

- 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.

"Designated threshold" refers to the amount set out in the Interpretative Notes.

"Financial institutions" means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   (a) money market instruments (cheques, bills, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;

---

5 This also captures private banking.

6 This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

7 This does not extend to financial leasing arrangements in relation to consumer products.

8 This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

(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.[9]

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 country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

"FIU" means financial intelligence unit.

"Legal arrangements" refers to express trusts or other similar legal arrangements.

"Legal persons" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

"Payable-through accounts" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political

9 *This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).*

party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

"Shell bank" means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

"STR" refers to suspicious transaction reports.

"Supervisors" refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

Annex

Interpretative Notes to The Forty Recommendations

"The FATF Recommendations" refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing.

Interpretative Notes

General Information

1. Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions".

2. Recommendations 5-16 and 21-22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

3. Where reference is made to a financial institution being satisfied as to a matter, that institution must be able to justify its assessment to competent authorities.

4. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.

5. The Interpretative Notes that apply to financial institutions are also relevant to designated nonfinancial businesses and professions, where applicable.

Recommendations 5, 12 and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as

follows:

- Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

RECOMMENDATION 5

Customer Due Diligence and Tipping Off

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

    a) Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.

    b) Make a STR to the FIU in accordance with Recommendation 13.

2. Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the

suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

CDD for Legal Persons and Arrangements

4. When performing elements (a) and (b) of the CDD process in relation to legal persons or arrangements, financial institutions should:

    a) Verify that any person purporting to act on behalf of the customer is so authorised, and identify that person.

    b) Identify the customer and verify its identity - the types of measures that would be normally needed to satisfactorily perform this function would require obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer's name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.

    c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

The relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

Reliance on Identification and Verification Already Performed

5. The CDD measures set out in Recommendation 5 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile.

Timing of Verification

6. Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:

    - Non face-to-face business.
    - Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
    - Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.

7. Financial institutions will also need to adopt risk management

procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions should refer to the Basel CDD paper[10] (section 2.2.6.) for specific guidance on examples of risk management measures for non-face to face business.

Requirement to Identify Existing Customers

8. The principles set out in the Basel CDD paper concerning the identification of existing customers should serve as guidance when applying customer due diligence processes to institutions engaged in banking activity, and could apply to other financial institutions where relevant.

Simplified or Reduced CDD Measures

9. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

10. Examples of customers where simplified or reduced CDD measures could apply are:

    - Financial institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.

10 "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.

- Public companies that are subject to regulatory disclosure requirements.
- Government administrations or enterprises.

11. Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements. Banks should also refer to the Basel CDD paper (section 2.2.4.), which provides specific guidance concerning situations where an account holding institution may rely on a customer that is a professional financial intermediary to perform the customer due diligence on his or its own customers (i.e. the beneficial owners of the bank account). Where relevant, the CDD Paper could also provide guidance in relation to similar accounts held by other types of financial institutions.

12. Simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

    - Life insurance policies where the annual premium is no more than USD/EUR 1000 or a single premium of no more than USD/EUR 2500.
    - Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.
    - A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

13. Countries could also decide whether financial institutions could apply these simplified measures only to customers in its own jurisdiction or allow them to do for customers from any other jurisdiction that the original country is satisfied is in compliance with and has effectively

implemented the FATF Recommendations.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

RECOMMENDATION 6

Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.

RECOMMENDATION 9

This Recommendation does not apply to outsourcing or agency relationships.

This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.

RECOMMENDATIONS 10 AND 11

In relation to insurance business, the word “transactions” should be understood to refer to the insurance product itself, the premium payment and the benefits.

RECOMMENDATION 13

1. The reference to criminal activity in Recommendation 13 refers to:

    a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or

    b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

    Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. In implementing Recommendation 13, suspicious transactions

should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state inter alia that their transactions relate to tax matters.

RECOMMENDATION 14 (TIPPING OFF)

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.

RECOMMENDATION 15

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.

RECOMMENDATION 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.

RECOMMENDATION 23

Recommendation 23 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.

RECOMMENDATION 25

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

RECOMMENDATION 26

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

RECOMMENDATION 27

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

RECOMMENDATION 38

Countries should consider:

a) Establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b) Taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

RECOMMENDATION 40

1. For the purposes of this Recommendation:

   - "Counterparts" refers to authorities that exercise similar responsibilities and functions.
   - "Competent authority" refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

2. Depending on the type of competent authority involved and the nature and purpose of the cooperation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial

transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports.
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.

The Forty Recommendations and Interpretative Notes are available at www.fatf-gafi.org/dataoecd/7/40/34849567.PDF

Financial Action Task Force — Special Recommendations on Terrorist Financing

Financial Action Task Force on Money Laundering
October 22, 2004

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and Implementation of UN Instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. CRIMINALISING THE FINANCING OF TERRORISM AND ASSOCIATED MONEY LAUNDERING

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. FREEZING AND CONFISCATING TERRORIST ASSETS

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. REPORTING SUSPICIOUS TRANSACTIONS RELATED TO TERRORISM

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

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.

VII. Wire Transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. NON-PROFIT ORGANISATIONS

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

(i) by terrorist organisations posing as legitimate entities;

(ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

(iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

IX. CASH COURIERS

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

Special Recommendations on Terrorist Financing are available at www.fatf-gafi.org/dataoecd/8/17/34849466.pdf

Basel Committee on Banking Supervision—Consolidated KYC Risk Management

October 2004

I. Introduction

1. The adoption of effective know-your-customer (KYC) standards is an essential part of banks' risk management practices. Banks with inadequate KYC risk management programmes may be subject to significant risks, especially legal and reputational risk. Sound KYC policies and procedures not only contribute to a bank's overall safety and soundness, they also protect the integrity of the banking system by reducing the likelihood of banks becoming vehicles for money laundering, terrorist financing and other unlawful activities. Recent initiatives to reinforce actions against terrorism in particular have underlined the importance of banks' ability to monitor their customers wherever they conduct business.

2. In October 2001, the Basel Committee on Banking Supervision (BCBS) issued Customer due diligence for banks ,subsequently reinforced by a General Guide to account opening and customer identification (CDD) in February 2003.

The CDD paper outlines four essential elements necessary for a sound KYC programme. These elements are: (i) customer acceptance policy; (ii) customer identification; (iii) on-going monitoring of higher risk accounts; and (iv) risk management. The principles laid down have been accepted and widely adopted by jurisdictions throughout the world as a benchmark for commercial banks and a good practice guideline for other categories of financial institution.

3. A key challenge in implementing sound KYC policies and procedures is how to put in place an effective groupwide approach. The legal and reputational risks identified in paragraph 1 are global in nature. As such, it is essential that each group develop a global risk management programme supported by policies that incorporate groupwide KYC standards. Policies and procedures at the branch-or subsidiary-level must be consistent with and supportive of the group KYC standards even where for local or business reasons such policies and procedures are not identical to the group's.

4. Consolidated KYC Risk Management means an established centralised process for coordinating and promulgating policies and procedures on a groupwide basis, as well as robust arrangements for the sharing of information within the group. Policies and procedures should be designed not merely to comply strictly with all relevant laws and regulations, but more broadly to identify, monitor and mitigate reputational, operational, legal and concentration risks. Similar to the approach to consolidated credit, market and operational risk, effective control of consolidated KYC risk requires banks to coordinate their risk management activities on a groupwide basis across the head office and all branches and subsidiaries.

5. The BCBS recognises that implementing effective KYC procedures on a groupwide basis is more challenging than many other risk management processes because KYC involves in most cases the liabilities rather than the assets side of the balance sheet, as well as balances that are carried as off-balance

sheet items. For reasons of customer privacy, some jurisdictions continue to restrict banks' ability to transmit names and balances as regards customer liabilities whereas there are now very few countries maintaining similar barriers on the assets side of the balance sheet. It is essential, in conducting effective monitoring on a groupwide basis, that banks be free to pass information about their liabilities or assets under management, subject to adequate legal protection, back to their head offices or parent bank. This applies in the case of both branches and subsidiaries. The conditions under which this might be achieved are set out in paragraphs [20 to 23].

6. Jurisdictions should facilitate consolidated KYC risk management by providing an appropriate legal framework which allows the cross-border sharing of information. Legal restrictions that impede effective consolidated KYC risk management processes should be removed.

II. Global process for managing KYC risks

7. The four essential elements of a sound KYC programme should be incorporated into a bank's risk management and control procedures to ensure that all aspects of KYC risk are identified and can be appropriately mitigated. Hence, a bank should aim to apply the same risk management, customer acceptance policy, procedures for customer identification, and process for monitoring its accounts throughout its branches and subsidiaries around the world. Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global KYC standards is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements In this regard banks should have robust information sharing between the head office and all branches and subsidiaries. Where the minimum KYC requirements of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two, subject to the direction given in CDD paragraph 66.

III. RISK MANAGEMENT

8. Groupwide KYC risk management programmes should include proper management oversight, systems and controls, segregation of duties, training and other related policies (CDD paragraph 55). The risk management programme should be implemented on a global basis. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures for the risk management programme are managed effectively and are in accordance with the bank's global standards for customer identification, ongoing monitoring of accounts and transactions and the sharing of relevant information.

9. Banks' compliance and internal audit staffs, or external auditors, should evaluate adherence to all aspects of their group's standards for KYC, including the effectiveness of centralised KYC functions and the requirements for sharing information with other group members and responding to queries from head office. Internationally active banking groups need both an internal audit and a global compliance function since these are the principal and in some circumstances the only mechanisms for monitoring the application of the bank's global KYC standards and supporting policies and procedures, including the effectiveness of the procedures for sharing information within the group.

IV. CUSTOMER ACCEPTANCE AND IDENTIFICATION POLICY

10. A bank should develop clear customer acceptance policies and procedures that include guidance on the types of customers that are likely to pose a higher than average risk to the bank (CDD paragraph 20), including managerial review of such prospective customers where appropriate.

11. Similarly, a bank should establish a risk-based systematic procedure for verifying the identity of new customers (CDD

paragraph 22). It should develop standards on what records are to be obtained and retained for customer identification on a global basis, including enhanced due diligence requirements for higher risk customers.

12. A bank should obtain appropriate identification information and maintain such information in a readily retrievable format so as to adequately identify its customers, as well as fulfil any local reporting requirements. Relevant information should be accessible for purposes of information sharing among the banking group's head office, branches and subsidiaries. Each office of the banking group should be in a position to comply with minimum identification and accessibility standards applied by the head office.

13. These customer acceptance, customer identification and record keeping standards should be implemented with consistent policies and procedures throughout the organisation, with adjustment as necessary to address variances in risk according to specific business line or geographic areas of operation. Moreover, it is recognised that different approaches to information collection and retention may be necessary across jurisdictions to conform with local regulatory requirements or relative risk factors.

V. Monitoring of accounts and transactions

14. An essential element for addressing higher risks is the coordinated approach to the monitoring of customer account activity on a groupwide basis, regardless of whether the accounts are held on- or

off-balance sheet, as assets under management, or on a fiduciary basis (CDD paragraph 16). Banks should have standards for monitoring account activity for potentially suspicious transactions that are implemented by supporting policies and procedures throughout its branches and subsidiaries worldwide. They should be risk-basedand emphasise the need to monitor material intra- and inter-country account activity.

15. Each office should maintain and monitor information on its accounts and transactions. This local monitoring should be complemented by a robust process of information sharing between the head office and its branches and subsidiaries regarding accounts and activity that may represent heightened risk.

16. In recent years, many banks have begun centralising certain processing systems and databases for internal risk management or efficiency purposes. In these circumstances, banks should complement local monitoring with transactions monitoring at the centralized site. This approach provides banks with the opportunity to monitor for patterns of suspicious activity that cannot be observed from the local site.

VI. GROUPWIDE INFORMATION SHARING

17. Banks should centralise the responsibility for coordinating groupwide information sharing. Subsidiaries and branches should be required to proactively provide information concerning higher risk customers and activities relevant to the global management of reputational and legal risks to, and respond to requests for account information from the head office or parent bank in a timely manner.

The bank's policies and procedures should include a description of the process to be followed for investigating and reporting potentially suspicious activity.

18. The bank's centralised KYC function should evaluate the potential risk posed by activity reported by its branches and subsidiaries and where appropriate assess its worldwide exposure to a given customer. The bank should have policies and procedures for ascertaining whether other branches or subsidiaries hold accounts for the same party and assessing the group-wide reputational, legal, concentration and operational risks. The bank should also have procedures governing global account relationships that are deemed potentially suspicious, detailing escalation procedures and guidance on restricting activities, including the closing of accounts as appropriate.

19. In addition, banks and their local offices should be responsive to requests from their respective law enforcement authorities for information about account holders that is needed in the authorities' effort to combat money laundering and the financing of terrorism. Head office should be able to require all offices to search their files against a list of individuals or organisations suspected of aiding and abetting terrorist financing or money laundering, and report matches.

VII. The role of the supervisor

20. Supervisors should verify that appropriate internal controls for KYC are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but

also a review of customer files and the sampling of accounts (CDD paragraph 61).

21. In a cross-border context, home country supervisors should face no impediments in verifying a branch or subsidiary's compliance with groupwide KYC policies and procedures during on-site inspections. This may well require a review of customer files and a sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. In the case of branches or subsidiaries of international banking groups, the host country supervisor retains responsibility for the supervision of compliance with local KYC regulations (which would include an evaluation of the appropriateness of the procedures).

22. The role of audit is particularly important in the evaluation of adherence to KYC standards on a consolidated basis and home country supervisors should ensure that appropriate frequency, resources and procedures are established in this regard and that they have full access to any relevant reports and working papers prepared through the audit process.

23. Safeguards are needed to ensure that information regarding individual accounts has the same confidentiality threshold afforded other information obtained through the supervisory process. A statement of mutual cooperation to facilitate information sharing between the two supervisors may well be helpful in this regard (CDD paragraph 68).

VIII. Legal impediments

24. Although gateways are in place in most jurisdictions to enable banks to share information with their head offices for risk management purposes, some countries have rigorous bank secrecy or data protection laws that prevent, or can be interpreted as preventing, the transfer of such information. In such circumstances, banks' overseas offices may be inclined to take a cautious stance regarding the transfer of customer information to their head offices which may conflict with the consolidated KYC objective.

25. It is essential that all jurisdictions that host foreign banks provide an appropriate legal framework which allows information for KYC risk management purposes to be passed to the head office/parent bank and home country supervisors. Similarly, there should be no impediments to onsite visits by head office auditors, risk managers, compliance officers or home country supervisors, nor any restrictions on their ability to access all the local office's records, including customers' names and balances. This access should be the same for both branches and subsidiaries. If impediments to information sharing prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question (CDD paragraph 69).

26. Where banks' head office staff are granted access to information on local customers, there should be no restrictions on them reporting such information back to head office. Such information should be subject to applicable privacy and privilege laws in the home country.

27. Subject to the conditions set out above, the BCBS believes that there is no justifiable reason why local legislation should impede the passage of customer information from a bank branch or subsidiary to its head office or parent bank for risk management purposes. If the law restricts disclosure of information to "third parties" it is essential that the head office or parent bank is clearly excluded from the definition of a third party. Jurisdictions that have legislation that impedes, or can be interpreted as impeding, such information sharing are urged to remove any such restrictions and to provide specific gateways.

IX. MIXED FINANCIAL GROUPS

28. Many banking groups now engage in securities and insurance businesses. Customer due diligence by mixed financial groups poses issues that may not be present for a pure banking group. Mixed groups should have systems and processes in place to monitor and share information on the identity of customers and account activity of the entire group, and to be alert to customers that use their services in different sectors. A customer relationship issue that arises in one part of a group would affect the reputational risk of the whole group.

29. While variations in the nature of activities, and patterns of relationships between institutions and customers in each sector justify variations in the KYC requirements imposed on each sector, the group should be alert when cross-selling products and services to customers from different business arms that the KYC requirements of the relevant sectors should be applied.

Basel Committee on Banking Supervision—Customer Due Diligence for Banks

October 2001

I. Introduction

1. Supervisors around the world are increasingly recognising the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

2. In reviewing the findings of an internal survey of cross-border banking in 1999, the Basel Committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries have significant gaps and in others they are non-existent. Even among countries with well-

developed financial markets, the extent of KYC robustness varies. Consequently, the Basel Committee asked the Working Group on Cross-border Banking[1] to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. The resulting paper was issued as a consultative document in January 2001. Following a review of the comments received, the Working Group has revised the paper and the Basel Committee is now distributing it worldwide in the expectation that the KYC framework presented here will become the benchmark for supervisors to establish national practices and for banks to design their own programmes. It is important to acknowledge that supervisory practices of some jurisdictions already meet or exceed the objective of this paper and, as a result, they may not need to implement any changes.

3. KYC is most closely associated with the fight against money-laundering, which is essentially the province of the Financial Action Task Force (FATF).[2] It is not the Committee's intention to duplicate the efforts of the FATF. Instead, the Committee's interest is from a wider prudential perspective. Sound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems. The Basel Committee and the Offshore Group of Banking Supervisors (OGBS) continue to support strongly the adoption and implementation of the FATF recommendations, particularly those relating to banks, and intend the standards in this paper to be consistent with the FATF recommendations. The Committee and the OGBS will also consider the adoption of any higher standards introduced by the FATF as a result of its current review of the 40 Recommendations. Consequently, the Working Group has been and will remain in close contact with the FATF as it develops its thoughts.

---

1 This is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

2 The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 31 member countries and two regional organisations. It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force. The FATF defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin.

4. The Basel Committee's approach to KYC is from a wider prudential, not just antimoney laundering, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

5. The Basel Committee's interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks' reputation significantly diminished had the banks maintained effective KYC programmes.

6. This paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/ or strengthened, by additional measures tailored to the risks of particular institutions and risks in the banking system of individual countries. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers. In a number of specific sections in this paper, there are recommendations for higher standards of due diligence for higher risk areas within a bank, where applicable.

7. The need for rigorous customer due diligence standards is not restricted to banks. The Basel Committee believes similar guidance needs to be developed for all non-bank financial institutions and professional intermediaries of financial services such as lawyers and accountants.

II. IMPORTANCE OF KYC STANDARDS FOR SUPERVISORS AND BANKS

8. The FATF and other international groupings have worked intensively on KYC issues, and the FATF's 40 Recommendations on combating money-laundering[3] have international recognition and application. It is not the intention of this paper to duplicate that work.

9. At the same time, sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

   - they help to protect banks' reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
   - they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

10. The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially **reputational, operational, legal and concentration risks**. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

11. **Reputational risk** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are

3 See FATF recommendations 10 to 19 which are reproduced in Annex 2.

especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

12. **Operational risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practise due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

13. **Legal risk** is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practise due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

14. Supervisory concern about **concentration risk** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

15. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of

funds by large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analysing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

16. Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.

17. Both the Basel Committee and the Offshore Group of Banking Supervisors are fully convinced that effective KYC practices should be part of the risk management and internal control systems in all banks worldwide. National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct[4] issued by industry organisations or associations can be of considerable value in underpinning regulatory guidance, by giving practical advice to banks on operational matters. However, such codes cannot be regarded as a substitute for formal regulatory guidance.

4 An example of an industry code is the "Global anti-money-laundering guidelines for Private Banking" (also called the Wolfsberg Principles) that was drawn up in October 2000 by twelve major banks with significant involvement in private banking.

III. ESSENTIAL ELEMENTS OF KYC STANDARDS

18. The Basel Committee's guidance on KYC has been contained in the following three papers and they reflect the evolution of the supervisory thinking over time. *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* issued in 1988 stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, decline suspicious transactions and cooperate with law enforcement agencies. The 1997 *Core Principles for Effective Banking Supervision* states, in a broader discussion of internal controls, that banks should have adequate policies, practices and procedures in place, including strict "know-your-customer" rules; specifically, supervisors should encourage the adoption of the relevant recommendations of the FATF. These relate to customer identification and record-keeping, increased diligence by financial institutions in detecting and reporting suspicious transactions, and measures to deal with countries with inadequate anti-money laundering measures. The 1999 Core Principles Methodology further elaborates the Core Principles by listing a number of essential and additional criteria. (Annex 1 sets out the relevant extracts from the *Core Principles and the Methodology*.)

19. All banks should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements".[5] Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by

5 *Core Principles Methodology, Essential Criterion 1.*

regular compliance reviews and internal audit. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

1. CUSTOMER ACCEPTANCE POLICY

20. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons (see section 2.2.3 below), should be taken exclusively at senior management level.

2. CUSTOMER IDENTIFICATION

21. Customer identification is an essential element of KYC standards. For the purposes of this paper, a customer includes:

- the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
- the beneficiaries of transactions conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

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.

23. Banks should "document and enforce policies for identification of customers and those acting on their behalf".[6] The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

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.[7] 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.

25. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

---

6 Core Principles Methodology, Essential Criterion 2.

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

26. Banks should develop "clear standards on what records must be kept on customer identification and individual transactions and their retention period".[8] Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. As the starting point and natural follow-up of the identification process, banks should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

2.1 General Identification Requirements

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. National supervisors are encouraged to provide guidance to assist banks in designing their own identification procedures. The Working Group intends to develop essential elements of customer identification requirements.

28. When an account has been opened, but problems of verification arise in the banking relationship which cannot be resolved, the bank should close the account and return the monies to the source from which they were received.[9]

29. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

8 Core Principles Methodology, Essential Criterion 2.

9 Subject to any national legislation concerning handling of suspicious transactions.

30. Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered[10] accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

2.2 SPECIFIC IDENTIFICATION ISSUES

31. There are a number of more detailed issues relating to customer identification which need to be addressed. Several of these are currently under consideration by the FATF as part of a general review of its 40 recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, Nominee and Fiduciary Accounts

32. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlors/grantors and beneficiaries.[11]

---

10 In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

11 Beneficiaries should be identified as far as possible when defined. It is recognised that it may not be possible to identify the beneficiaries of trusts precisely at the outset. For example, some beneficiaries may be unborn children and some may be conditional on the occurrence of specific events. In addition, beneficiaries being specific classes of individuals (e.g. employee pension funds) may be appropriately dealt with as pooled accounts as referred to n paragraphs 38-9.

2.2.2 Corporate Vehicles

33. Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies, may make proper identification of customers or beneficial owners difficult. A bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

34. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies needs to be obtained. In the case of entities which have a significant proportion of capital in the form of bearer shares, extra vigilance is called for. A bank may be completely unaware that the bearer shares have changed hands. The onus is on banks to put in place satisfactory procedures to monitor the identity of material beneficial owners. This may require the bank to immobilise the shares, e.g. by holding the bearer shares in custody.

2.2.3 Introduced Business

35. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

36. The Basel Committee recommends that banks that use introducers should carefully assess whether the introducers are "fit and proper"

and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:[12]

- 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.

2.2.4 Client Accounts Opened By Professional Intermediaries

37. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

38. Banks often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension

12 The FATF is currently engaged in a review of the appropriateness of eligible introducers.

funds and money funds. Banks also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

39. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the bank. National supervisory guidance should clearly set out those circumstances in which banks need not look beyond the intermediary. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the bank should apply the criteria set out in paragraph 36 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

40. Where the intermediary is not empowered to furnish the required information on beneficiaries to the bank, for example, lawyers[13] bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this paper or to the requirements of comprehensive anti-money laundering legislation, then the bank should not permit the intermediary to open an account.

2.2.5 Politically Exposed Persons

41. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such

13 The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients.

politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

42. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

43. Some countries have recently amended or are in the process of amending their laws and regulations to criminalise active corruption of foreign civil servants and public officers in accordance with the relevant international convention.[14] In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for a bank considering a relationship with a person whom it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

14 See OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, adopted by the Negotiating Conference on 21 November 1997.

44. Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.

2.2.6 Non-Face-to-Face Customers

45. Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of nonface- to-face customer identification is being discussed by the FATF, and is also under review in the context of amending the 1991 EEC Directive.

46. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.[15]

47. Even though the same documentation can be provided by face-to-face and nonface- to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers. With telephone and electronic banking, the verification problem is made even more difficult.

---

15 The Electronic Banking Group of the Basel Committee issued a paper on risk management principles for electronic banking in May 2001.

48. In accepting business from non-face-to-face customers:

- banks should apply equally effective customer identification procedures for nonface- to-face customers as for those available for interview; and
- there must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- certification of documents presented;
- requisition of additional documents to complement those which are required for face-to-face customers;
- independent contact with the customer by the bank;
- third party introduction, e.g. by an introducer subject to the criteria established in paragraph 36; or
- requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

2.2.7 Correspondent Banking

49. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

50. Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and

its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

51. In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "noncooperative" in the fight against anti-money laundering. Banks should establish that their respondent banks have due diligence standards as set out in this paper, and employ enhanced due diligence procedures with respect to transactions carried out though the correspondent accounts.

52. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 36.

3. ON-GOING MONITORING OF ACCOUNTS AND TRANSACTIONS

53. On-going monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs

to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be very helpful to banks and should be included as part of a jurisdiction's anti-moneylaundering procedures and/or guidance.

54. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

- Senior management in charge of private banking business should know the personal circumstances of the bank's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager.

- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them.[16] As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

4. RISK MANAGEMENT

55. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively and are, at a minimum, in accordance with local supervisory practice. The channels for reporting suspicious transactions should be clearly specified in writing, and communicated to all personnel. There should also be internal procedures for assessing whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and and/or supervisory authorities.

56. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff

16 *It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations, etc. It should however be noted that PEPs (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, masking the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.*

performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

57. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that audit functions are staffed adequately with individuals who are wellversed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

58. All banks must have an ongoing employee-training programme so that bank staff are adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within banks that promotes such understanding is the key to successful implementation.

59. In many countries, external auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

IV. THE ROLE OF SUPERVISORS

60. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as presented in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice.

61. In addition to setting out the basic elements for banks to follow, supervisors have a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Supervisors should ensure that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts. Supervisors should always have the right to access all documentation related to accounts maintained in that jurisdiction, including any analysis the bank has made to detect unusual or suspicious transactions.

62. Supervisors have a duty not only to ensure their banks maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system.[17] Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures and regulatory requirements. In addition, supervisors should ensure that banks are aware of and pay particular attention to transactions that involve jurisdictions where standards are considered inadequate. The FATF and some national authorities have listed a number of countries and jurisdictions that are considered to have legal and administrative arrangements that do not comply with international standards for combating money laundering. Such findings should be a component of a bank's KYC policies and procedures.

---

17 Many supervisors also have a duty to report any suspicious, unusual or illegal transactions that they detect, for example, during onsite examinations.

V. IMPLEMENTATION OF KYC STANDARDS IN A CROSS-BORDER CONTEXT

63. Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a groupwide basis. This is a challenging task for banks and supervisors alike.

64. Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for their inspection. As far as compliance checks are concerned, supervisors and external auditors should in most cases examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

65. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

66. Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a bank from adopting standards that are higher than the minima required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavours to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent bank and its home country supervisor are fully informed of the nature of the difference.

67. Criminal elements are likely to be drawn toward jurisdictions with such impediments. Hence, banks should be aware of the high reputational risk of conducting business in these jurisdictions. Parent banks should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

68. During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. This will require a review of customer files and some random sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. Where the home country supervisor requires consolidated reporting of deposit or borrower concentrations or notification of funds under management, there should be no impediments. In addition, with a view to monitoring deposit concentrations or the funding risk of the deposit being withdrawn, home supervisors may apply materiality tests and establish some thresholds so that if a customer's deposit exceeds a certain percentage of the balance sheet, banks should report it to the home supervisor. However, safeguards are needed to ensure

that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation[18] to facilitate information sharing between the two supervisors would be helpful in this regard.

69. In certain cases there may be a serious conflict between the KYC policies of a parent bank imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or home country supervisors, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor should communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially. If they prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question. In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements may be helpful. Access to information by home country supervisors should be as unrestricted as possible, and at a minimum they should have free access to the banks' general policies and procedures for customer due diligence and for dealing with suspicions.

18 See the Basel Committee paper Essential elements of a statement of cooperation between banking supervisors (May 2001).

Annex 1

EXCERPTS FROM "CORE PRINCIPLES METHODOLOGY"

Principle 15: Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, by criminal elements.

Note: *A new draft "consultative" version of this document was published by the Basel Committee on Banking Supervision in April 2006. In the new version, Know Your Customer issues are addressed in Principle 18, "Abuse of Financial Services."*

ESSENTIAL CRITERIA

1. The supervisor determines that banks have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. This includes the prevention and detection of criminal activity or fraud, and reporting of such suspected activities to the appropriate authorities.

2. The supervisor determines that banks have documented and enforced policies for identification of customers and those acting on their behalf as part of their antimoney- laundering program. There are clear rules on what records must be kept on customer identification and individual transactions and the retention period.

3. The supervisor determines that banks have formal procedures to recognise potentially suspicious transactions. These might include additional authorisation for large cash (or similar) deposits or withdrawals and special procedures for unusual transactions.

4. The supervisor determines that banks appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local statutory and regulatory anti-money laundering requirements.

5. The supervisor determines that banks have clear procedures, communicated to all personnel, for staff to report suspicious transactions to the dedicated senior officer responsible for anti-money laundering compliance.

6. The supervisor determines that banks have established lines of communication both to management and to an internal security (guardian) function for reporting problems.

7. In addition to reporting to the appropriate criminal authorities, banks report to the supervisor suspicious activities and incidents of fraud material to the safety, soundness or reputation of the bank.

8. Laws, regulations and/or banks' policies ensure that a member of staff who reports suspicious transactions in good faith to the dedicated senior officer, internal security function, or directly to the relevant authority cannot be held liable.

9. The supervisor periodically checks that banks' money laundering controls and their systems for preventing, identifying and reporting fraud are sufficient. The supervisor has adequate enforcement powers (regulatory and/or criminal prosecution) to take action against a bank that does not comply with its anti-money laundering obligations.

10. The supervisor is able, directly or indirectly, to share with domestic and foreign financial sector supervisory authorities information related to suspected or actual criminal activities.

11. The supervisor determines that banks have a policy statement on ethics and professional behaviour that is clearly communicated to all staff.

ADDITIONAL CRITERIA

1. The laws and/or regulations embody international sound practices, such as compliance with the relevant forty Financial Action Task Force Recommendations issued in 1990 (revised 1996).

2. The supervisor determines that bank staff is adequately trained on money laundering detection and prevention.

3. The supervisor has the legal obligation to inform the relevant criminal authorities of any suspicious transactions.

4. The supervisor is able, directly or indirectly, to share with relevant judicial authorities information related to suspected or actual criminal activities.

5. If not performed by another agency, the supervisor has in-house resources with specialist expertise on financial fraud and anti-money laundering obligations.

Annex 2

EXCERPTS FROM FATF RECOMMENDATIONS

C. ROLE OF THE FINANCIAL SYSTEM IN COMBATING MONEY LAUNDERING

Customer Identification and Record-Keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

    In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

    (i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

    (ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial

operation in the country where their registered office is located).

12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

    Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

    These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

13. Countries should 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.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

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.

16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for

breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

    (i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

    (ii) an ongoing employee training programme;

    (iii) an audit function to test the system.

Customer Due Diligence for Banks is available at www.bis.org/publ/bcbs85.html

Wolfsberg Statement on Monitoring Screening and Searching

September 2003

1. Preamble

The Wolfsberg Group of financial institutions (the "Wolfsberg Group")1 has previously produced: Global Anti-Money Laundering Guidelines for Private Banking; The Wolfsberg Statement on The Suppression of the Financing of Terrorism; and The Wolfsberg Anti-Money Laundering Principles for Correspondent Banking. All of these have stated the need for appropriate monitoring of transactions and customers to identify potentially unusual or suspicious activity and transactions, and for reporting such to competent authorities. The Guidelines, Statement and Principles, however, have not addressed issues related to the development of risk-based processes for monitoring, screening and searching of transactions and customers. Therefore, the Wolfsberg Group is making this statement to identify issues that should be addressed in order that financial institutions are able to develop suitable monitoring, screening and searching processes.

The Wolfsberg Group acknowledges that the risk profile may be different for a financial institution as a whole and for its individual units depending on the business conducted in a particular unit (e.g. Retail, Private Banking, Correspondent Banking, Broker Dealer). It must be recognised, however, that any process for

monitoring, screening or searching is limited to detecting those clients and transactions that have identifiable characteristics that are distinguishable from apparently legitimate behaviour. Because money launderers and terrorists will take all available actions to attempt to disguise their transactions and accounts by providing them with an air of legitimacy, it becomes difficult, if not sometimes impossible, to make any distinctions between good and bad clients and acceptable and potentially illicit transactions. We are, however, committed to implementing processes and methods and making use of information technology systems where appropriate, so that we, to the best of our ability, have in place efficient and effective processes and systems to identify potential suspicious activity.

2. DEFINITIONS

- Real-time Screening (Screening): Defined as the screening or filtering of payment instructions (i.e. wire or funds transfers) prior to their execution in order to prevent making funds available in breach of sanctions, embargoes and other measures.
- Retroactive Searches (Searches): Defined as the identification of specific past transactions, as well as existing and closed accounts.
- Transaction Monitoring (Monitoring): Defined as the process of monitoring transactions after their execution in order to identify unusual transactions, including monitoring single transactions, as well as transaction flows.

3. ROLE OF FINANCIAL INSTITUTIONS

Financial institutions must have appropriate processes in place that allow for the identification of unusual activity and unusual patterns of activity or transactions. Since unusual transactions, patterns or activity need not be suspicious in all cases, financial institutions must have the ability to analyse and determine if the

activity, patterns or transactions are suspicious in nature with regard to, among other things, potential money laundering. Suspicious activity, patterns and transactions must be reported to competent authorities in accordance with local laws, regulations or rules.

Monitoring of account activity and transactions flowing through a financial institution is one means of ensuring that this role is fulfilled. Financial institutions should have processes in place to screen payment instructions against the lists provided by competent governmental authorities to identify amongst others, potential terrorists or terrorist financing. Financial institutions should respond expeditiously to search requests from competent governmental authorities.

4. Risk-Based Approach

Traditionally, laws, regulations and rules with regard to monitoring, screening and searching issued by some governmental authorities have not embraced a risk-based approach. Instead governmental directives have focused on collecting data from financial institutions by establishing thresholds, such as large cash transaction reports, or by providing specific information on which financial institutions must react, such as embargoes or sanctions. Implicit in these collection and reporting obligations is that activity or transactions that are being reported may be suspicious or illegal. However, because, for example, not all large transactions are suspicious, monitoring should not be limited to focusing on thresholds, but rather should be aimed at recognising unusual activity in comparison to known and expected activities.

Similar to the risk-based approach for conducting due diligence at account opening, monitoring, and some screening and searching processes should also be risk-based. A risk-based approach for monitoring and relevant screening and searching should be closely linked to the risk-based approach used at account opening and such an approach should consider both elements that increase as well as reduce risk. Where financial institutions know their clients better, including understanding their intended activity at the institution, the greater is the ability to identify gaps between current activity and past and expected activities, which in turn provides financial institutions with critical information to assist in determining whether unusual or suspicious activity exists.

Financial institutions should consider the use of information technology systems

in the context of the risk associated with the business units, e.g. size, nature of business conducted and overall monitoring process.

Therefore, a risk-based approach may require a differentiated level of implementation of real-time screening, retroactive searches and transaction monitoring systems.

4.1 Real-time Screening

Real-time transaction screening is the screening or filtering of payment instructions (i.e. wire or funds transfers) prior to their execution. Real-time screening is typically used for enforcing embargoes and sanctions. Real-time screening can be most effectively used for the identification of payments to or from persons or entities for which governmental authorities have provided notice to financial institutions. While it is crucial that screening is undertaken on a real-time basis in order to block affected payments before completion, it can adversely affect Straight Through Processing and, therefore, requires timely action on the part of governmental authorities in order to allow appropriate payments to be completed within the time periods specified by the clearing and settlement systems.

In order to enhance the quality of real-time screening, the Wolfsberg Group believes that the following points are of utmost importance:

- real-time screening should only be required to be used for screening or filtering related to embargoes or sanctions, and financial institutions should not be required to engage in real-time screening for names other than those specified by relevant governmental authorities;
- real-time screening technology should be driven by responses that only require a true or false answer to matches with the applicable lists provided by governmental authorities;
- financial institutions should be able to rely on the quality and completeness of the names provided by governmental authorities; and
- criteria should be established as to acceptable amounts and types of information that must be provided to financial institutions to conduct real-time screening to include such

things as, full name, date of birth and other relevant unique identifiers which should mitigate the significant number of "false positives" (i.e. apparent matches that prove incorrect on substantive review).

4.2 Retroactive Searches

Retroactive searches may be the result of ongoing risk-based due diligence or enhanced due diligence pursuant to policies and procedures implemented by financial institutions. Retroactive searches may also be the result of requests by governmental authorities or the issuance of judicial processes, such as subpoenas or search warrants, that require financial institutions to search for specific data.

The Wolfsberg Group believes that retroactive searches provide a valuable tool for locating and identifying transactions and accounts of interest. However, there is not uniformity among financial institutions and governmental authorities as to how retroactive searches should be conducted and what records at an

institution should be the subject of such searches. The lack of uniformity and clarity can (and often does) lead to time consuming manual searches.

When financial institutions engage in retroactive searches as the result of their own processes, care should be taken to ensure that such searches are risk-based. Financial institutions should identify those data sources that will allow for the most effective and efficient searches to identify the appropriate data based on the risks associated with the customer or transactions.

As a means of developing uniformity that will provide necessary assistance to financial institutions and ultimately produce retroactive searches of significant utility to law enforcement activities, the Wolfsberg Group recommends that governmental authorities, in consultation with financial institutions, identify specific types of data that it would be of value to maintain electronically (e.g. client identifying information, beneficial owner information, transaction information) and financial institutions should seek to create such information in an electronic format that would then support effective and efficient retroactive searches.

4.3 Transaction Monitoring

The majority of ongoing monitoring for unusual and potentially suspicious activity is accomplished by transaction monitoring. Risk-based transaction monitoring

for potential money laundering requires the development of risk models that identify the potential risks to money laundering and provide a means of ranking the risks in order to compare the risks to completed transactions. An appropriate transaction monitoring process will compare the transaction information against the identified risks, such as geographic location of transaction, the type of products and services being offered and the type of client engaging in the transaction with the different typologies for money laundering and other ilicit activites to determine if a transaction is unusual or suspicious.

This approach requires that a model exist that supports the identification of transactions that deviate from a standard model or benchmark and allows a risk-based review and analysis. Transaction monitoring based on such a concept provides financial institutions with the necessary coverage for review of transactions that are not subject to real-time screening or retroactive searches. The Wolfsberg Group intends to continue to develop guidance for

- a process that permits reasonable reviewing of transactions;
- identifying reasonable, risk-based scores / alerts;
- ensuring comparability between financial institutions as to the robustness of the model;
- establishing industry standards for understanding levels or degrees of “unusualness” or suspicion; and
- ability to replace or enhance current process of monitoring solely for transactions exceeding specific thresholds.

5. STANDARDS FOR RISK-BASED TRANSACTION MONITORING

An effective risk-based transaction monitoring process should:

- compare the client’s account/transaction history to the client’s specific profile information and a relevant peer

group and/or compare the clients account/transaction history against established money laundering criteria/ scenarios, in order to identify patterns of suspicious activity or anomalies

- establish a process to compare customer or transaction specific data against risk scoring models;
- be capable of recognizing patterns and of "learning" which transactions are normal for a client rather than designating certain transactions as unusual (for example, not all large transaction are unusual and may easily be explained);
- issue alerts if unusual transactions are identified;
- track those alerts in order to ensure that they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required;
- maintain an audit trail for inspection by the institution's audit function and by bank supervisors; and
- provide appropriate aggregated information and statistics.

6. CONCLUSION

Risk-based transaction monitoring, real-time screening and retroactive searches must be embedded in an integrated anti-money laundering program. Past experience indicates that those current governmental standards for monitoring for suspicious activity, which have tended not to be risk-based, are not effective enough for identifying potential money laundering activity. The Wolfsberg Group believes that a risk-based approach will enhance the effectiveness of monitoring unusual or potentially suspicious activity, to the extent such activity is distinguishable from legitimate activity. It is for this reason that the Wolfsberg Group supports the introduction of risk-based monitoring models that set forth uniform standards or baselines while being sufficiently flexible to meet the needs of individual financial institutions. The Wolfsberg Group is committed to the development of appropriate standards and benchmarks towards establishing effective risk-based monitoring, screening and searching models.

Wolfsberg Anti-Money Laundering Principles for Correspondent Banking

November 2002

1. Preamble

The Wolfsberg Group of International Financial Institutions[1] has agreed that these Principles constitute global guidance on the establishment and maintenance of Correspondent Banking relationships. The Wolfsberg Group believes that adherence to these Principles will further effective risk management and enable institutions to exercise sound business judgement with respect to their clients. Furthermore, adherence to these Principles will support the aim of Wolfsberg Group members to prevent the use of their worldwide operations for criminal purposes.

2. Correspondent Banking

These Principles extend to all Correspondent Banking relationships an institution establishes or maintains for another Correspondent Banking Client.[2] Correspondent Banking is the

1 The Wolfsberg Group consists of the following leading international financial institutions: ABN AMRO Bank N.V., Banco Santander Central Hispano S.A., Bank of Tokyo-Mitsubishi Ltd., Barclays Bank, Citigroup, Credit Suisse Group, Deutsche Bank AG, Goldman Sachs, HSBC, J. P. Morgan Chase, Société Générale, UBS AG.

provision of a current or other liability account and related services to another institution used to meet its cash clearing, liquidity management and short-term borrowing or investment needs. Institutions may decide to extend these Principles to all relationships that they maintain with financial institutions.

3. RESPONSIBILITY AND OVERSIGHT

The institution shall define policies and procedures that require specified personnel to be responsible for ensuring compliance with these Principles. The policies and procedures shall require that at least one person senior to or independent from the officer sponsoring the relationship approve the Correspondent Banking relationship. The policies and procedures also shall provide for independent review by appropriate personnel to ensure continued compliance with the institution's policies and procedures and these Principles.

4. RISK-BASED DUE DILIGENCE

These Principles advocate a risk-based approach. Correspondent Banking Clients presenting greater risk should be subjected to a higher level of due diligence. These Principles outline the type of risk indicators that an institution shall consider in initiating the relationship, and on a continuing basis, to ascertain what reasonable due diligence or enhanced due diligence it will undertake. In particular, the institution will consider these risk indicators:

- **The Correspondent Banking Client's Domicile** — The jurisdiction where the Correspondent Banking Client is based and/or where its ultimate parent is headquartered may present greater risk. Certain jurisdictions are internationally recognised as having inadequate anti-money laundering standards, insufficient regulatory supervision,

2 *Correspondent Banking Client is a client of an institution that is a financial services firm that uses the institution's Correspondent Banking services accounts to clear transactions for its own client base. The term includes (but is not limited to) Banks, Broker-Dealers, Mutual Funds, Unit Trusts, Investment Services Firms, Hedge Funds, Introducing Brokers, Money Service Businesses, Pension Funds, Credit Card Providers, Commercial Credit Companies, Household Finance Companies, Mortgage Banks, Building Societies and Leasing Companies.*

or presenting greater risk for crime, corruption or terrorist financing. On the other hand, other jurisdictions such as members of the Financial Action Task Force (FATF) have more robust regulatory environments representing lower risks. Institutions will review pronouncements from regulatory agencies and international bodies, such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the Correspondent Banking Client is based and/or in which its ultimate parent is headquartered.

- **The Correspondent Banking Client's Ownership and Management Structures** — The location of owners, their corporate legal form and the transparency of ownership structure may present greater risks. Similarly, the location and experience of management may raise additional concerns. The involvement of Politically Exposed Persons (PEP) in the management or ownership of certain Correspondent Banking Clients may also increase the risk. PEPs are individuals who have or have had positions of public trust such as government officials, senior executives of government corporations, politicians, important political party officials etc. and their families and close associates.

- **The Correspondent Banking Client's Business and Customer Base** — The type of businesses the Correspondent Banking Client engages in, as well as the type of the markets the Correspondent Banking Client serves, may present greater risks. Involvement in certain business segments internationally recognised as creating particular vulnerability to money laundering, corruption or terrorist financing presents additional concern. Consequently, a Correspondent Banking Client that derives a substantial part of its business income from Higher Risk Clients may present greater risk. Higher Risk Clients are those clients of a Correspondent Banking Client that may be involved in activities or are connected to jurisdictions that are identified by credible sources as activities or countries being especially susceptible to money laundering.

Each institution may give the appropriate weight to each risk factor as it deems necessary.

5. DUE DILIGENCE STANDARDS

All Correspondent Banking Clients shall be subjected to appropriate due diligence that will seek to assure that an institution is comfortable conducting business with a particular client given the client's risk profile. It may be appropriate for an institution to consider the fact that a Correspondent Banking Client operates in or is subjected to a regulatory environment that is internationally recognised as adequate in the fight against money laundering. In these instances, an institution may also rely on publicly available information obtained either from the Correspondent Banking Client or reliable third parties (regulators, exchanges, etc.) to satisfy its due diligence requirements. In conducting due diligence on any Correspondent Banking Client, the elements set out below shall be considered, as appropriate.

- **Client Domicile and Organisation**

  The jurisdiction where the Correspondent Banking Client's ultimate parent is incorporated and/or headquartered and where the particular operating unit wishing to maintain the relationship conducts its business, as well as the corporate legal form of the Correspondent Banking Client.

- **Client Ownership and Executive Management**

  Whether the Correspondent Banking Client is publicly held or privately owned; whether if publicly held, its shares are traded on an exchange in a jurisdiction with an adequately recognised regulatory scheme; and the identity of any significant controlling interests. The structure and experience of Executive Management. These are the most senior executives in charge of its day- to-day business. Depending on the circumstances of the Correspondent Banking Client this may include the Members of the Correspondent Banking Client's Board of Directors or Supervisory Board or Executive Committee or its Executive Committee or its equivalent. The existence of any PEP in the Executive Management or ownership structure.

- **Correspondent Banking Client's Business**

  The types of financial products and services the Correspondent Banking Client offers to its own clients, and depending upon the risk associated with the Correspondent Banking Client, the geographic markets reached.

- **Products or Services Offered**

  The business purpose(s) for the relationship with the Correspondent Banking Client, including the products and services offered to the Correspondent Banking Client.

- **Regulatory Status and History**

  The primary regulatory body responsible for overseeing or supervising the Correspondent Banking Client. If circumstances warrant, an institution will also consider publicly available materials to ascertain whether the Correspondent Banking Client has been the subject of any criminal or adverse regulatory action in the recent past.

- **Anti-Money Laundering Controls**

  The nature of the Correspondent Banking Client's anti-money laundering controls and the extent to which they are globally applied.

- **No Business Arrangements With Shell Banks**

  Confirm that the Correspondent Banking Clients will not use the institution's products and services to engage in business with Shell Banks.

  A Shell Bank is a bank that: (i) does not conduct business at a fixed address in a jurisdiction in which the Shell Bank is authorised to engage in banking activities; (ii) does not employ one or more individuals on a full time business at this fixed address; (iii) does not maintain operating records at this address; and (iv) is not subject to inspection by the banking authority that licensed it to conduct banking activities. A bank which meets these requirements but which is also a Regulated Affiliate is not a Shell Bank for the purposes of these Principles. A Regulated Affiliate is a bank which would

otherwise be a Shell Bank or an Offshore Bank (as the case may be) but which is owned, directly or indirectly by a financial institution that is licensed in a jurisdiction that is not a FATF Non-cooperative Jurisdiction and which is subject to supervision by the banking authority of that jurisdiction.

- **Client Visit**

  Unless other measures suffice, a representative of the Institution should visit the Correspondent Banking Client at their premises prior to or within a reasonable period of time after establishing a relationship with an Correspondent Banking Client, amongst other things to confirm that the Correspondent Banking Client is not a Shell Bank.

6. ENHANCED DUE DILIGENCE

In addition to due diligence, each institution will also subject those Correspondent Banking Clients that present greater risks to enhanced due diligence.

The enhanced due diligence process will involve further consideration of the following elements designed to assure the institution has secured a greater level of understanding:

- **Ownership and Management**

  For all significant controlling interests, the owners' sources of wealth and background, including their reputation in the market place, as well as recent material ownership changes (e.g. in the last five years). Similarly, a more detailed understanding of the experience of each member of the Executive Management as well as recent material changes in the Executive Management structure (e.g. within the last two years).

- **PEP Involvement**

  If a PEP appears to have an interest or management role in a Correspondent Banking Client, then the institution shall ensure it has an understanding of that person's role in the Correspondent Banking Client.

- **Correspondent Banking Client's Anti-Money Laundering Controls**

  The quality of the Correspondent Banking Client's anti-money laundering and client identification controls including whether these controls meet internationally recognised standards. The extent to which an institution will enquire will depend upon the risks presented. Additionally, the institution may speak with representatives of the Correspondent Banking Client to obtain comfort that the Correspondent Banking Client's senior management recognise the importance of anti-money laundering controls.

- **Downstream Correspondent Clearing**

  A Downstream Correspondent Clearer is a Correspondent Banking Client who receives Correspondent Banking services from an institution and itself provides Correspondent Banking services to other financial institutions in the same currency as the account it maintains with the institution. When these services are offered to an Correspondent Banking Client that is itself a Downstream Correspondent Clearer, the institution will take reasonable steps to understand the types of financial institutions to whom the Correspondent Banking Client offers the Downstream Correspondent services and consider the degree to which the Correspondent Banking Client examines the anti-money laundering controls of the financial institutions to whom it offers those services.

7. SHELL BANKS

An institution will not offer its products or services to a Shell Bank.

8. Central Banks and Supra-National Organisations

These Principles shall generally not apply to relationships with central banks and monetary authorities of FATF-Member Countries or Supra-national, Regional Development or Trade Banks (e.g. European Bank for Reconstruction and Development, International Monetary Fund, the World Bank), at least insofar as the relationship with that entity involves the provision of products and services that are in keeping with that entity's primary activities.

9. Branches, Subsidiaries and Affiliates

The determination of the level and scope of due diligence that is required on a Correspondent Banking Client shall be made after considering the relationship between the Correspondent Banking Client and its ultimate parent (if any). In general, in situations involving branches, subsidiaries or affiliates, the parent of the Correspondent Banking Client shall be considered in determining the extent of required due diligence. In instances when the Correspondent Banking Client is an affiliate that is not substantively and effectively controlled by the parent, then both the parent and Correspondent Banking Client shall be reviewed. However, certain facts unique to the branch, subsidiary or affiliate may dictate that enhanced due diligence be performed.

10. Application to Client Base

Institutions will apply these Principles to new Correspondent Banking Clients. Additionally, as these Principles unify concepts that may not have previously been applied globally, each institution will undertake a risk-based review of their existing base of Correspondent Banking Clients to determine whether additional due diligence is necessary to achieve the level of understanding espoused by these Principles.

11. UPDATING CLIENT FILES

The institution's policies and procedures shall require that the Correspondent Banking Client information is reviewed and updated on a periodic basis or when a material change in the risk profile of the Correspondent Banking Client occurs. Periodic review of the Correspondent Banking Clients will occur on a risk-assessed basis.

12. MONITORING AND REPORTING OF SUSPICIOUS ACTIVITIES

The institution shall implement bank-wide policies and procedures to detect and investigate unusual or suspicious activity and report as required by applicable law. These will include guidance on what is considered to be unusual or suspicious and give examples thereof. The policies and procedures shall include appropriate monitoring of the Correspondent Banking activity.

13. INTEGRATION WITH ANTI-MONEY LAUNDERING PROGRAMME

These Principles shall form an integral component of the institution's wider anti-money laundering programme.

14. RECOMMENDATION FOR AN INTERNATIONAL REGISTRY

The Wolfsberg Group encourages the development and regulatory endorsement of an international registry for financial institutions. Upon registering financial institutions would submit information useful for conducting due diligence as outlined in these Principles. Financial institutions would rely on this information in adhering to these Principles.

Anti-Money Laundering Principles for Correspondent Banking is available at www.wolfsberg-principles.com/corresp-banking.html

Wolfsberg Statement on the Suppression of the Financing of Terrorism

January 2002

1. Preamble

The Wolfsberg Group of financial institutions (the "Wolfsberg Group" (1)) is committed to contributing to the fight against terrorism and is making the following statement to describe the role of financial institutions in preventing the flow of terrorist funds through the world's financial system.

This fight presents new challenges. Funds used in the financing of terrorism do not necessarily derive from criminal activity, which is a requisite element of most existing money laundering offences. Successful participation in this fight by the financial sector requires global cooperation by governments with the financial institutions to an unprecedented degree.

---

1 This is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

2 The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 31 member countries and two regional organisations. It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force. The FATF defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin.

2. ROLE OF FINANCIAL INSTITUTIONS IN THE FIGHT AGAINST TERRORISM

Financial institutions can assist governments and their agencies in the fight against terrorism. They can help this effort through prevention, detection and information sharing. They should seek to prevent terrorist organizations from accessing their financial services, assist governments in their efforts to detect suspected terrorist financing and promptly respond to governmental enquiries.

3. RIGHTS OF THE INDIVIDUAL

The Wolfsberg Group is committed to participating in the fight against terrorism in a manner which is non-discriminatory and is respectful of the rights of individuals.

4. KNOW YOUR CUSTOMER

The Wolfsberg Group recognises that adherence to existing "Know Your Customer" policies and procedures is important to the fight against terrorism. Specifically the proper identification of customers by financial institutions can improve the efficacy of searches against lists of known or suspected terrorists issued by competent authorities having jurisdiction over the relevant financial institution ("applicable lists").

In addition to the continued application of existing customer identification, acceptance and due diligence procedures, the Wolfsberg Group is committed to:

- Implementing procedures for consulting applicable lists and taking reasonable and practicable steps to determine whether a person involved in a prospective or existing business relationship appears on such a list.

3 See FATF recommendations 10 to 19 which are reproduced in Annex 2.

- Reporting to the relevant authorities matches from lists of known or suspected terrorists or terrorist organisations consistent with applicable laws and regulations regarding the disclosure of customer information.
- Exploring with governmental agencies ways of improving information exchange within and between jurisdictions.
- Exploring ways of improving the maintenance of customer information to facilitate the timely retrieval of such information.

5. HIGH RISK SECTORS AND ACTIVITIES

The Wolfsberg Group is committed to applying enhanced and appropriate due diligence in relation to those of their customers engaged in sectors and activities which have been identified by competent authorities as being widely used for the financing of terrorism, such as underground banking businesses or alternative remittance systems. This will include the adoption, to the extent not already in place, of specific policies and procedures on acceptance of business from customers engaged in such sectors or activities, and increased monitoring of activity of customers who meet the relevant acceptance criteria.

In particular the Wolfsberg Group is committed to restricting their business relationships with remittance businesses, exchange houses, casas de cambio, bureaux de change and money transfer agents to those which are subject to appropriate regulation aimed at preventing such activities and businesses from being used as a conduit to launder the proceeds of crime and/or finance terrorism.

The Wolfsberg Group recognises that many jurisdictions are currently in the process of developing and implementing regulations with regard to these businesses and that appropriate time needs to be given for these regulations to take effect.

6. MONITORING

Recognising the difficulties inherent in identifying financial transactions linked to the financing of terrorism (many of which appear routine in relation to information known at the time) the Wolfsberg Group is committed to the continued application of existing monitoring procedures for identifying unusual or suspicious transactions. The Wolfsberg Group recognises that while the motive for such transactions may be unclear, monitoring and then identifying and reporting unusual or suspicious transactions may assist government agencies by linking seemingly unrelated activity
to the financing of terrorism.

In addition, the Wolfsberg Group is committed to:

- Exercising heightened scrutiny in respect of customers engaged in sectors identified by competent authorities as being widely used for the financing of terrorism.
- Monitoring account and transactional activity (to the extent meaningful information is available to financial institutions) against lists generated by competent authorities of known or suspected terrorists or terrorist organisations.
- Working with governments and agencies in order to recognise patterns and trends identified as related to the financing of terrorism.
- Considering the modification of existing monitoring procedures as necessary to assist in the identification of such patterns and trends.

7. NEED FOR ENHANCED GLOBAL CO-OPERATION

The Wolfsberg Group is committed to co-operating with and assisting law enforcement and government agencies in their efforts to combat the financing of terrorism. The Wolfsberg Group has identified the following areas for discussion with governmental agencies, with a view to enhancing the contribution financial institutions are able to make:

- The provision of official lists of suspected terrorists and terrorist organisations on a globally co-ordinated basis by the relevant competent authority in each jurisdiction.
- The inclusion of appropriate details and information in official lists to assist financial institutions in efficient and timely searches of their customer bases. This information should ideally include (where known) in the case of individuals: date of birth; place of birth; passport or identity card number; in the case of corporations; place of incorporation or establishment; details of principals; to the extent possible, reason for inclusion on the list; and geographic information, such as the location, date and time of the transaction.
- Providing prompt feedback to financial institutions on reports made following circulation of such official lists.
- The provision of meaningful information in relation to patterns, techniques and mechanisms used in the financing of terrorism to assist with monitoring procedures.
- The provision of meaningful information about corporate and other types of vehicles used to facilitate terrorist financing.
- The development of guidelines on appropriate levels of heightened scrutiny in relation to sectors or activities identified by competent authorities as being widely used for terrorist financing.
- The development by governments and clearing agencies of uniform global formats for funds transfers that require information which may assist their efforts to prevent and detect the financing of terrorism.
- Ensuring that national legislation:
    - Permits financial institutions to maintain information derived from official lists within their own databases and to share such information within their own groups.
    - Affords financial institutions protection from civil liability for relying on such lists.
    - Permits financial institutions to report unusual or suspicious transactions that may relate to terrorism to the relevant

authorities without breaching any duty of customer confidentiality or privacy legislation.

- Permits the prompt exchange of information between governmental agencies of different nation states.

The Wolfsberg Group supports the FATF Special Recommendations on Terrorist Financing as measures conducive to the suppression of the financing of terrorism.

Wolfsberg Anti-Money Laundering Principles on Private Banking

Revised May 2002

Preamble

The following guidelines are understood to be appropriate for private banking relationships. Guidelines for other market segments may differ. It is recognized that the establishment of policies and procedures to adhere to these guidelines is the responsibility of management.

1. Client Acceptance: General Guidelines

1.1 General

Bank policy will be to prevent the use of its worldwide operations for criminal purposes. The bank will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate. The primary responsibility for this lies with the private banker who sponsors

the client for acceptance. Mere fulfilment of internal review procedures does not relieve the private banker of this basic responsibility.

1.2 IDENTIFICATION

The bank will take reasonable measures to establish the identity of its clients and beneficial owners and will only accept clients when this process has been completed.

1.2.1 CLIENT

- Natural persons: identity will be established to the bank's satisfaction by reference to official identity papers or such other evidence as may be appropriate under the circumstances.
- Corporations, partnerships, foundations: the bank will receive documentary evidence of the due organization and existence.
- Trusts: the bank will receive appropriate evidence of formation and existence along with identity of the trustees.
- Identification documents must be current at the time of opening.

1.2.2 BENEFICIAL OWNER

Beneficial ownership must be established for all accounts. Due diligence must be done on all principal beneficial owners identified in accordance with the following principles:

- Natural persons: when the account is in the name of an individual, the private banker must establish whether the client is acting on his/her own behalf. If doubt exists, the bank will establish the capacity in which and on whose behalf the accountholder is acting.
- Legal entities: where the client is a company, such as a private investment company, the private banker will understand the structure of the company sufficiently to determine the provider of funds, principal owner(s) of the shares and those who have control over the funds, e.g. the directors and those with the power to give direction to

the directors of the company. With regard to other shareholders the private banker will make a reasonable judgement as to the need for further due diligence. This principle applies regardless of whether the share capital is in registered or bearer form.

- Trusts: where the client is a trustee, the private banker will understand the structure of the trust sufficiently to determine the provider of funds (e.g. settlor) those who have control over the funds (e.g. trustees) and any persons or entities who have the power to remove the trustees. The private banker will make a reasonable judgement as to the need for further due diligence.

- Unincorporated associations: the above principles apply to unincorporated associations.

- The bank will not permit the use of its internal non-client accounts (sometimes referred to as "concentration" accounts) to prevent association of the identity of a client with the movement of funds on the client's behalf, i.e., the bank will not permit the use of such internal accounts in a manner that would prevent the bank from appropriately monitoring the client's account activity.

1.2.3 Accounts Held in the Name of Money Managers and Similar Intermediaries

The private banker will perform due diligence on the intermediary and establish that the intermediary has a due diligence process for its clients, or a regulatory obligation to conduct such due diligence, that is satisfactory to the bank.

1.2.4 Powers of Attorney/Authorized Signers

Where the holder of a power of attorney or another authorized signer is appointed by a client, it is generally sufficient to do due diligence on the client.

1.2.5 PRACTICES FOR WALK-IN CLIENTS AND ELECTRONIC BANKING RELATIONSHIPS

A bank will determine whether walk-in clients or relationships initiated through electronic channels require a higher degree of due diligence prior to account opening. The bank will specifically address measures to satisfactorily establish the identity of non-face-to-face customers.

1.3 DUE DILIGENCE

It is essential to collect and record information covering the following categories:

- Purpose and reasons for opening the account
- Anticipated account activity
- Source of wealth (description of the economic activity which has generated the net worth)
- Estimated net worth
- Source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening)
- References or other sources to corroborate reputation information where available.

Unless other measures reasonably suffice to do the due diligence on a client (e.g. favorable and reliable references), a client will be met prior to account opening.

1.4 NUMBERED OR ALTERNATE NAME ACCOUNTS

Numbered or alternate name accounts will only be accepted if the bank has established the identity of the client and the beneficial owner. These accounts must be open to a level of scrutiny by the bank's appropriate control layers equal to the level of scrutiny applicable to other client accounts.

1.5 OFFSHORE JURISDICTIONS

Risks associated with entities organized in offshore jurisdictions are covered by due diligence procedures laid out in these guidelines.

1.6 OVERSIGHT RESPONSIBILITY

There will be a requirement that all new clients and new accounts be approved by at least one person other than the private banker.

2 CLIENT ACCEPTANCE: SITUATIONS REQUIRING ADDITIONAL DILIGENCE/ ATTENTION

2.1 GENERAL

In its internal policies, the bank must define categories of persons whose circumstances warrant additional diligence. This will typically be the case where the circumstances are likely to pose a higher than average risk to a bank.

2.2 INDICATORS

The circumstances of the following categories of persons are indicators for defining them as requiring additional diligence:

- Persons residing in and/or having funds sourced from countries identified by credible sources as having inadequate anti- money laundering standards or representing high risk for crime and corruption.
- Persons engaged in types of business activities or sectors known to be susceptible to money laundering.
- “Politically Exposed Persons” (frequently abbreviated

as “PEPs”), referring to individuals holding or having held positions of public trust, such as government officials, senior executives of government corporations, politicians, important political party officials, etc., as well as their families and close associates.

2.3 SENIOR MANAGEMENT APPROVAL

The banks’ internal policies should indicate whether, for any one or more among these categories, senior management must approve entering into new relationships.

Relationships with Politically Exposed Persons may only be entered into with the approval from senior management.

3 UPDATING CLIENT FILES

3.1

The private banker is responsible for updating the client file on a defined basis and/or when there are major changes. The private banker’s supervisor or an independent control person will review relevant portions of client files on a regular basis to ensure consistency and completeness. The frequency of the reviews depends on the size, complexity and risk posed of the relationship.

3.2

With respect to clients classified under any category of persons mentioned in 2, the banks internal policies will indicate whether senior management must be involved in these reviews.

3.3

Similarly, with respect to clients classified as set forth in 3.2, the bank's internal policies will indicate what management information must be provided to management and/or other control layers. The policies should also address the frequency of these information flows.

3.4

The reviews of PEPs must require senior management's involvement.

4 PRACTICES WHEN IDENTIFYING UNUSUAL OR SUSPICIOUS ACTIVITIES

4.1 DEFINITION OF UNUSUAL OR SUSPICIOUS ACTIVITIES

The bank will have a written policy on the identification of and follow-up on unusual or suspicious activities. This policy will include a definition of what is considered to be suspicious or unusual and give examples thereof.

Unusual or suspicious activities may include:

- Account transactions or other activities which are not consistent with the due diligence file
- Cash transactions over a certain amount
- Pass-through / in-and-out-transactions.

4.2 IDENTIFICATION OF UNUSUAL OR SUSPICIOUS ACTIVITIES UNUSUAL OR SUSPICIOUS ACTIVITIES CAN BE IDENTIFIED THROUGH:

- Monitoring of transactions
- Client contacts (meetings, discussions, in-country visits etc.)
- Third party information (e.g. newspapers, Reuters, internet)
- Private banker's / internal knowledge of the client's environment (e.g. political situation in his/her country).

4.3 FOLLOW-UP ON UNUSUAL OR SUSPICIOUS ACTIVITIES

The private banker, management and/or the control function will carry out an analysis of the background of any unusual or suspicious activity. If there is no plausible explanation a decision will be made involving the control function:

- To continue the business relationship with increased monitoring
- To cancel the business relationship
- To report the business relationship to the authorities.

The report to the authorities is made by the control function and senior management may need to be notified (e.g. Senior Compliance Officer, CEO, Chief Auditor, General Counsel). As required by local laws and regulations the assets may be blocked and transactions may be subject to approval by the control function.

5 MONITORING

5.1 MONITORING PROGRAM

A sufficient monitoring program must be in place. The primary responsibility for monitoring account activities lies with the private banker. The private banker will be familiar with significant transactions and increased activity in the account and will be especially aware of unusual or suspicious activities (see 4.1). The bank will decide to what extent fulfillment of these responsibilities will need to be supported through the use of automated systems or other means.

5.2 ONGOING MONITORING

With respect to clients classified under any category of persons mentioned in 2, the bank's internal policies will indicate how the account activities will be subject to monitoring.

6 CONTROL RESPONSIBILITIES

A written control policy will be in place establishing standard control procedures to be undertaken by the various "control layers" (private banker, independent operations unit, Compliance, Internal Audit). The control policy will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow-up, etc.

An independent audit function (which may be internal to the bank) will test the programs contemplated by the control policy.

7 REPORTING

There will be regular management reporting established on money laundering issues (e.g. number of reports to authorities, monitoring tools, changes in applicable laws and regulations, the number and scope of training sessions provided to employees).

8 EDUCATION, TRAINING AND INFORMATION

The bank will establish a training program on the identification and prevention of money laundering for employees who have client contact and for Compliance personnel. Regular training (e.g. annually) will also include how to identify and follow-up on unusual or suspicious activities. In addition, employees will be informed about any major changes in anti-money-laundering laws and regulations.

All new employees will be provided with guidelines on the anti-money-laundering procedures.

9 RECORD RETENTION REQUIREMENTS

The bank will establish record retention requirements for all anti-money-laundering related documents. The documents must be kept for a minimum of five years.

10 EXCEPTIONS AND DEVIATIONS

The bank will establish an exception and deviation procedure that requires risk assessment and approval by an independent unit.

11 ANTI-MONEY LAUNDERING ORGANIZATION

The bank will establish an adequately staffed and independent department responsible for the prevention of money laundering (e.g. Compliance, independent control unit, Legal).

Anti-Money Laundering Principles on Private Banking is available at www.wolfsberg-principles.com/privat-banking.html

OF 26 OCTOBER 2005 ON THE PREVENTION OF THE USE OF THE FINANCIAL SYSTEM FOR THE PURPOSE OF MONEY LAUNDERING AND TERRORIST FINANCING

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 47 (2), first and third sentences, and Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and

Social Committee[1],

Having regard to the opinion of the European Central Bank[2],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[3],

1 Opinion delivered on 11 May 2005 (not yet published in the Official Journal).
2 OJ C 40, 17.2.2005, p. 9.
3 Opinion of the European Parliament of 26 May 2005 (not yet published in the Official Journal) and Council Decision of 19 September 2005.

Whereas:

(1) Massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.

(2) The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to avoid Member States' adopting measures to protect their financial systems which could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Community public policy, Community action in this area is necessary.

(3) In order to facilitate their criminal activities, money launderers and terrorist financers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, if certain coordinating measures are not adopted at Community level.

(4) In order to respond to these concerns in the field of money laundering, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [4] was adopted. It required Member States to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions, to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities.

(5) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even Community level, without taking account of international

4 OJ L 166, 28.6.1991, p. 77. Directive as amended by Directive 2001/97/EC of the European Parliament and of the Council (OJL 344, 28.12.2001, p. 76).

coordination and cooperation, would have very limited effects. The measures adopted by the Community in this field should therefore be consistent with other action undertaken in other international fora. The Community action should continue to take particular account of the Recommendations of the Financial Action Task Force (hereinafter referred to as the FATF), which constitutes the foremost international body active in the fight against money laundering and terrorist financing. Since the FATF Recommendations were substantially revised and expanded in 2003, this Directive should be in line with that new international standard.

(6) The General Agreement on Trade in Services (GATS) allows Members to adopt measures necessary to protect public morals and prevent fraud and adopt measures for prudential reasons, including for ensuring the stability and integrity of the financial system.

(7) Although initially limited to drugs offences, there has been a trend in recent years towards a much wider definition of money laundering based on a broader range of predicate offences. A wider range of predicate offences facilitates the reporting of suspicious transactions and international cooperation in this area. Therefore, the definition of serious crime should be brought into line with the definition of serious crime in Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime[5]. 25.11.2005 L 309/15 Official Journal of the European Union EN

(8) Furthermore, the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures of this Directive should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes.

(9) Directive 91/308/EEC, though imposing a customer identification obligation, contained relatively little detail on the

5 OJ L 182, 5.7.2001, p. 1.

relevant procedures. In view of the crucial importance of this aspect of the prevention of money laundering and terrorist financing, it is appropriate, in accordance with the new international standards, to introduce more specific and detailed provisions relating to the identification of the customer and of any beneficial owner and the verification of their identity. To that end a precise definition of 'beneficial owner' is essential. Where the individual beneficiaries of a legal entity or arrangement such as a foundation or trust are yet to be determined, and it is therefore impossible to identify an individual as the beneficial owner, it would suffice to identify the class of persons intended to be the beneficiaries of the foundation or trust. This requirement should not include the identification of the individuals within that class of persons.

(10) The institutions and persons covered by this Directive should, in conformity with this Directive, identify and verify the identity of the beneficial owner. To fulfil this requirement, it should be left to those institutions and persons whether they make use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measures relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.

(11) Credit agreements in which the credit account serves exclusively to settle the loan and the repayment of the loan is effected from an account which was opened in the name of the customer with a credit institutioncovered by this Directive pursuant to Article 8(1)(a) to(c) should generally be considered as an example of types of less risky transactions.

(12) To the extent that the providers of the property of alegal entity or arrangement have significant control over the use of the property they should be identified as abeneficial owner.

(13) Trust relationships are widely used in commercial products as an internationally recognised feature of the comprehensively supervised wholesale financial markets. An obligation to identify the beneficial owner does not arise from the fact alone that there is a trust relationship in this particular case.

(14) This Directive should also apply to those activities of the institutions and persons covered hereunder which are performed on the Internet.

(15) As the tightening of controls in the financial sector has prompted money launderers and terrorist financers to seek alternative methods for concealing the origin of the proceeds of crime and as such channels can be used for terrorist financing, the anti-money laundering and antiterrorist financing obligations should cover life insurance intermediaries and trust and company service providers.

(16) Entities already falling under the legal responsibility of an insurance undertaking, and therefore falling within the scope of this Directive, should not be included within the category of insurance intermediary.

(17) Acting as a company director or secretary does not of itself make someone a trust and company service provider. For that reason, the definition covers only those persons that act as a company director or secretary for a third party and by way of business.

(18) The use of large cash payments has repeatedly proven to be very vulnerable to money laundering and terrorist financing. Therefore, in those Member States that allow cash payments above the established threshold, all natural or legal persons trading in goods by way of business should be covered by this Directive when accepting such cash payments. Dealers in high-value goods, such as precious stones or metals, or works of art, and auctioneers are in any event covered by this Directive to the extent that payments to them are made in cash in an amount of EUR 15 000 or more. To ensure effective monitoring of compliance with this Directive by that potentially wide group of institutions and persons, Member States may focus their monitoring activities in particular on those natural and legal persons trading in goods that are exposed to a relatively high risk of money laundering or terrorist financing, in accordance with the principle of risk-based supervision. In view of the different situations in the various Member States, Member States may decide to adopt stricter provisions, in order to properly address the risk involved with large cash payments.

(19) Directive 91/308/EEC brought notaries and other independent legal professionals within the scope of the Community anti-money laundering regime; this coverage should be maintained unchanged in this Directive; these legal professionals, as defined by the Member States, are subject to the provisions of this Directive when participating in financial or corporate transactions, including providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing.

(20) Where independent members of professions providing legal advice which are legally recognised and controlled, such as lawyers, are ascertaining the legal position of a client or representing a client in legal proceedings, it would not be appropriate under this Directive to put those legal professionals in respect of these activities under an obligation to report suspicions of money laundering or terrorist financing. There must be exemptions from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position for a client. Thus, legal advice shall remain subject to the obligation of professional secrecy unless the legal counsellor is taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.

(21) Directly comparable services need to be treated in the same manner when provided by any of the professionals covered by this Directive. In order to ensure the respect of the rights laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Treaty on European Union, in the case of auditors, external accountants and tax advisors, who, in some Member States, may defend or represent a client in the context of judicial proceedings or ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to the reporting obligations in accordance with this Directive.

(22) It should be recognised that the risk of money laundering and terrorist financing is not the same in every case. In line with a risk-based approach, the principle should be introduced into Community legislation that simplified customer due diligence is allowed in appropriate cases.

(23) The derogation concerning the identification of beneficial owners of pooled accounts held by notaries or other independent legal professionals should be without prejudice to the obligations that those notaries or other independent legal professionals have pursuant to this Directive. Those obligations include the need for such notaries or other independent legal professionals themselves to identify the beneficial owners of the pooled accounts held by them.

(24) Equally, Community legislation should recognise that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.

(25) This is particularly true of business relationships with individuals holding, or having held, important public positions, particularly those from countries where corruption is widespread. Such relationships may expose the financial sector in particular to significant reputational and/or legal risks. The international effort to combat corruption also justifies the need to pay special attention to such cases and to apply the complete normal customer due diligence measures in respect of domestic politically exposed persons or enhanced customer due diligence measures in respect of politically exposed persons residing in another Member State or in a third country.

(26) Obtaining approval from senior management for establishing business relationships should not imply obtaining approval from the board of directors but from the immediate higher level of the hierarchy of the person seeking such approval.

(27) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate,

subject to suitable safeguards, to allow customers to be introduced whose identification has been carried out elsewhere. Where an institution or person covered by this Directive relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the institution or person to whom the customer is introduced. The third party, or introducer, also retains his own responsibility for all the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

(28) In the case of agency or outsourcing relationships on a contractual basis between institutions or personscovered by this Directive and external natural or legal persons not covered hereby, any anti-money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the institutions or persons covered by this Directive, may only arise from contract and not from this Directive. The responsibility for complying with this Directive should remain with the institution or person covered hereby.

(29) Suspicious transactions should be reported to the financial intelligence unit (FIU), which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIUs, allowing them to conduct their business properly, including international cooperation with other FIUs.

(30) By way of derogation from the general prohibition on executing suspicious transactions, the institutions and persons covered by this Directive may execute suspicious transactions before informing the competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice

to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(31) Where a Member State decides to make use of the exemptions provided for in Article 23(2), it may allow or require the self-regulatory body representing the persons referred to therein not to transmit to the FIU any information obtained from those persons in the circumstances referred to in that Article.

(32) There has been a number of cases of employees who report their suspicions of money laundering being subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of the anti-money laundering and anti-terrorist financing system. Member States should be aware of this problem and should do whatever they can to protect employees from such threats or hostile action.

(33) Disclosure of information as referred to in Article 28 should be in accordance with the rules on transfer of personal data to third countries as laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1]. Moreover, Article 28 cannot interfere with national data protection and professional secrecy legislation.

(34) Persons who merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution do not fall within the scope of this Directive, nor does any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settlement systems.

(35) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Community credit and financial institutions have branches and

1 OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

subsidiaries located in third countries where the legislation in this area is deficient, they should, in order to avoid the application of very different standards within an institution or group of institutions, apply the Community standard or notify the competent authorities of the home Member State if this application is impossible.

(36) It is important that credit and financial institutions should be able to respond rapidly to requests for information on whether they maintain business relationships with named persons. For the purpose of identifying such business relationships in order to be able to provide that information quickly, credit and financial institutions should have effective systems in place which are commensurate with the size and nature of their business. In particular it would be appropriate for credit institutions and larger financial institutions to have electronic systems at their disposal. This provision is of particular importance in the context of procedures leading to measures such as the freezing or seizing of assets (including terrorist assets), pursuant to applicable national or Community legislation with a view to combating terrorism.

(37) This Directive establishes detailed rules for customer due diligence, including enhanced customer due diligence for high-risk customers or business relationships, such as appropriate procedures to determine whether a person is a politically exposed person, and certain additional, more detailed requirements, such as the existence of compliance management procedures and policies. All these requirements are to be met by each of the institutions and persons covered by this Directive, while Member States are expected to tailor the detailed implementation of those provisions to the particularities of the various professions and to the differences in scale and size of the institutions and persons covered by this Directive.

(38) In order to ensure that the institutions and others subject to Community legislation in this field remain committed, feedback should, where practicable, be made available to them on the usefulness and follow-up of the reports they present. To make this possible, and to be able to review the effectiveness of their systems to combat money laundering and terrorist financing Member States should keep and improve the relevant statistics.

(39) When registering or licensing a currency exchange office, a trust and company service provider or a casino nationally, competent authorities should ensure that the persons who effectively direct or will direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should be established in conformity with national law. As a minimum, such criteria should reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

(40) Taking into account the international character of money laundering and terrorist financing, coordination and cooperation between FIUs as referred to in Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information[1], including the establishment of an EU FIU-net, should be encouraged to the greatest possible extent. To that end, the Commission should lend such assistance as may be needed to facilitate such coordination, including financial assistance.

(41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive penalties in national law for failure to respect the national provisions adopted pursuant to this Directive. Provision should be made for penalties in respect of natural and legal persons. Since legal persons are often involved in complex money laundering or terrorist financing operations, sanctions should also be adjusted in line with the activity carried on by legal persons.

(42) Natural persons exercising any of the activities referred to in Article 2(1)(3)(a) and (b) within the structure of a legal person, but on an independent basis, should be independently responsible for compliance with the provisions of this Directive, with the exception of Article 35.

(43) Clarification of the technical aspects of the rules laid down in this Directive may be necessary to ensure an effective and

1 OJ L 271, 24.10.2000, p. 4.

sufficiently consistent implementation of this Directive, taking into account the different financial instruments, professions and risks in the different Member States and the technical developments in the fight against money laundering and terrorist financing. The Commission should accordingly be empowered to adopt implementing measures, such as certain criteria for identifying low and high risk situations in which simplified due diligence could suffice or enhanced due diligence would be appropriate, provided that they donot modify the essential elements of this Directive and provided that the Commission acts in accordance with the principles set out herein, after consulting the Committee on the Prevention of Money Laundering and Terrorist Financing.

(44) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[2]. To that end a new Committee on the Prevention of Money Laundering and Terrorist Financing, replacing the Money Laundering Contact Committee set up by Directive 91/308/EEC, should be established.

(45) In view of the very substantial amendments that would need to be made to Directive 91/308/EEC, it should be repealed for reasons of clarity.

(46) Since the objective of this Directive, namely the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective. 5.11.2005 L 309/19 Official Journal of the European Union EN

(47) In exercising its implementing powers in accordance with this Directive, the Commission should respect the following principles:

2 OJ L 184, 17.7.1999, p. 23.

the need for high levels of transparency and consultation with institutions and persons covered by this Directive and with the European Parliament and the Council; the need to ensure that competent authorities will be able to ensure compliance with the rules consistently; the balance of costs and benefits to institutions and persons covered by this Directive on a long-term basis in any implementing measures; the need to respect the necessary flexibility in the application of the implementing measures in accordance with a risk-sensitive approach; the need to ensure coherence with other Community legislation in this area; the need to protect the Community, its Member States and their citizens from the consequences of money laundering and terrorist financing.

(48) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the European Convention on Human Rights.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

1. Member States shall ensure that money laundering and terrorist financing are prohibited.

2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting

any person who is involved in the commission of such activity to evade the legal consequences of his action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

4. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision2002/475/JHA of 13 June 2002 on combating terrorism[1].

5. Knowledge, intent or purpose required as an element of the activities mentioned in paragraphs 2 and 4 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to:

(1) credit institutions;

(2) financial institutions;

1 OJ L 164, 22.6.2002, p. 3.

(3) the following legal or natural persons acting in the exerciseof their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting 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 necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(c) trust or company service providers not already covered under points (a) or (b);

(d) real estate agents;

(e) other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;

(f) casinos.

2. Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited

basis and where there is little risk of money laundering or terrorist financing occurring do not fall within the scope of

Article 3 (1) or (2).

Article 3

For the purposes of this Directive the following definitions shall apply:

(1) 'credit institution' means a credit institution, as defined in the first subparagraph of Article 1(1) of Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions[1], including branches within the meaning of Article 1(3) of that Directive located in the Community of credit institutions having their head offices inside or outside the Community;

(2) 'financial institution' means:

(a) an undertaking other than a credit institution which carries out one or more of the operations included in points 2 to 12 and 14 of Annex I to Directive 2000/12/EC, including the activities of currency exchange offices (bureaux de change) and of money transmission or remittance offices;

(b) an insurance company duly authorised in accordance with Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance[2], insofar as it carries out activities covered by that Directive;

(c) an investment firm as defined in point 1 of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments[3];

(d) a collective investment undertaking marketing its units or shares;

1 OJ L 126, 26.5.2000, p. 1. Directive as last amended by Directive 2005/1/EC (OJ L 79, 24.3.2005, p. 9).
2 OJ L 345, 19.12.2002, p. 1. Directive as last amended by Directive 2005/1/EC.
3 OJ L 145, 30.4.2004, p. 1.

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation[4], with the exception of intermediaries as mentioned in Article 2(7) of that Directive, when they act in respect of life insurance and other investment related services;

(f) branches, when located in the Community, of financial institutions as referred to in points (a) to (e), whose head offices are inside or outside the Community;

(3) 'property' means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of a serious crime;

(5) 'serious crimes' means, at least:

(a) acts as defined in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(b) any of the offences defined in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union[5];

(d) fraud, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities' Financial Interests[6];

(e) corruption;

4 OJ L 9, 15.1.2003, p. 3.
5 OJ L 351, 29.12.1998, p. 1.
6 OJ C 316, 27.11.1995, p. 49.

(f) all offences which are punishable by deprivation ofliberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

(6) 'beneficial owner' means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;

(ii) the natural person(s) who otherwise exercises control over the management of a legal entity:

(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

(i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;

(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity;

(7) 'trust and company service providers' means any natural or legal person which by way of business provides any of the following services to third parties:

(a) forming companies or other legal persons;

(b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

(d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;

(e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards;

(8) 'politically exposed persons' means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;

(9) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this Directive and which is expected, at the time when the contact is established, to have an element of duration;

(10) 'shell bank' means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Article 4

1. Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the institutions and persons referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing.

CHAPTER II

CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

Article 6

Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks. By way of derogation from Article 9(6), Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be made the subject of customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

Article 7

The institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 8

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

(c) obtaining information on the purpose and intended nature of the business relationship;

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

2. The institutions and persons covered by this Directive shall apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The institutions and persons covered by this Directive shall be able to demonstrate to the competent authorities mentioned in Article 37, including self-regulatory bodies, that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

Article 9

1. Member States shall require that the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying-out of the transaction.

2. By way of derogation from paragraph 1, Member States may allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

3. By way of derogation from paragraphs 1 and 2, Member States may, in relation to life insurance business, allow the verification of the identity of the beneficiary under the policy to take place after the business relationship has been established. In that case, verification shall take place at or before the time of payout or at or before the time the beneficiary intends to exercise rights vested under the policy.

4. By way of derogation from paragraphs 1 and 2, Member States may allow the opening of a bank account provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the aforementioned provisions is obtained.

5. Member States shall require that, where the institution or person concerned is unable to comply with points (a), (b) and (c) of Article 8(1), it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or shall terminate the business relationship, and shall consider making a report to the financial intelligence unit (FIU) in accordance with Article 22 in relation to the customer. Member States shall not be obliged to apply the previous subparagraph in situations when notaries, independent legal professionals, auditors, external accountants and tax advisors are in the course of ascertaining the legal position for their client or performing their

task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.25.11.2005 L 309/23 Official Journal of the European Union EN

6. Member States shall require that institutions and persons covered by this Directive apply the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

Article 10

1. Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of EUR 2 000 or more.

2. Casinos subject to State supervision shall be deemed in any event to have satisfied the customer due diligence requirements if they register, identify and verify the identity of their customers immediately on or before entry, regardless of the amount of gambling chips purchased.

SECTION 2

Simplified customer due diligence

Article 11

1. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), the institutions and persons covered by this Directive shall not be subject to the requirements provided for in those Articles 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 requirements equivalent to those laid down in this Directive and supervised for compliance with those requirements.

2. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1) Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

(a) listed companies whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation;

(b) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts;

(c) domestic public authorities, or in respect of any other customer representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

3. In the cases mentioned in paragraphs 1 and 2, institutions and persons covered by this Directive shall in any case gather sufficient information to establish if the customer qualifies for an exemption as mentioned in these paragraphs.

4. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 1 or 2 or in other situations which meet the technical criteria established in accordance with Article 40(1)(b).

5. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence

in respect of:

(a) life insurance policies where the annual premium is no more than EUR 1 000 or the single premium is no morethan EUR 2 500;

(b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; 25.11.2005 L 309/24 Official Journal of the European Union EN

(d) electronic money, as defined in Article 1(3)(b) of 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 institutions[1], where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Article 3 of Directive 2000/46/EC, or in respect of any other product or transaction representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

Article 12

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the institutions and persons covered by this Directive from applying simplified due diligence to credit and financial institutions or listed companies from the third country concerned or other entities following from situations which meet the technical criteria established in accordance with Article 40(1)(b).

1 OJ L 275, 27.10.2000, p. 39.

SECTION 3

Enhanced customer due diligence

Article 13

1. Member States shall require the institutions and persons covered by this Directive to apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the measures referred to in Articles 7, 8 and 9(6), in situations which by their nature can present a higher risk of money laundering or terrorist financing, and at least in the situations set out in paragraphs 2, 3, 4 and in other situations representing a high risk of money laundering or terrorist financing which meet the technical criteria established in accordance with Article 40(1)(c).

2. Where the customer has not been physically present for identification purposes, Member States shall require those institutions and persons to take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures:

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by this Directive;

(c) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

3. In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, Member States shall require their credit institutions to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly

available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;

(c) obtain approval from senior management before establishing new correspondent banking relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

4. In respect of transactions or business relationships with politically exposed persons residing in another Member State or in a third country, Member States shall require those institutions and persons covered by this Directive to:

(a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person;

(b) have senior management approval for establishing business relationships with such customers;

(c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

(d) conduct enhanced ongoing monitoring of the business relationship.

5. Member States shall prohibit credit institutions from entering into or continuing a correspondent banking relationship with a shell bank and shall require that credit institutions take appropriate measures to ensure that they do not engage in or continue

correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

6. Member States shall ensure that the institutions and persons covered by this Directive pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

SECTION 4

Performance by third parties

Article 14

Member States may permit the institutions and persons covered by this Directive to rely on third parties to meet the requirements laid down in Article 8(1)(a) to (c). However, the ultimate responsibility for meeting those requirements shall remain with the institution or person covered by this Directive which relies on the third party.

Article 15

1. Where a Member State permits credit and financial institutions referred to in Article 2(1)(1) or (2) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit institutions and persons referred to in Article 2(1) situated in its territory to recognise and accept, in accordance with the provisions laid down in Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by an institution referred to in Article 2(1)(1) or (2) in another Member State, with the exception of currency exchange offices and money transmission or remittance offices, and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

2. Where a Member State permits currency exchange offices and money transmission or remittance offices referred to in Article 3(2)(a) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by the same category of institution in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

3. Where a Member State permits persons referred to in Article 2(1)(3)(a) to (c) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by a person referred to in Article 2(1)(3)(a) to (c) in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

Article 16

1. For the purposes of this Section, 'third parties' shall mean institutions and persons who are listed in Article 2, or equivalent institutions and persons situated in a third country, who meet the following requirements:

(a) they are subject to mandatory professional registration, recognised by law;

(b) they apply customer due diligence requirements and record keeping requirements as laid down or equivalent to those laid down in this Directive and their compliance with the requirements of this Directive is supervised in accordance with Section 2 of Chapter V, or they are

situated in a third country which imposes equivalent requirements to those laid down in this Directive.

2. Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraph 1(b).

Article 17

Where the Commission adopts a decision pursuant to Article 40(4), Member States shall prohibit the institutions and persons covered by this Directive from relying on third parties from the third country concerned to meet the requirements laid down in Article 8(1)(a) to (c).

Article 18

1. Third parties shall make information requested in accordance with the requirements laid down in Article 8(1)(a) to (c) immediately available to the institution or person covered by this Directive to which the customer is being referred.

2. Relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner shall immediately be forwarded, on

request, by the third party to the institution or person covered by this Directive to which the customer is being referred.

Article 19

This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the institution or person covered by this Directive.

CHAPTER III

REPORTING OBLIGATIONS

SECTION 1

General provisions

Article 20

Member States shall require that the institutions and persons covered by this Directive pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Article 21

1. Each Member State shall establish a FIU in order effectively to combat money laundering and terrorist financing.

2. That FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation. It shall be provided with adequate resources in order to fulfil its tasks.

3. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks.

Article 22

1. Member States shall require the institutions and persons covered by this Directive, and where applicable their directors and employees, to cooperate fully:

(a) by promptly informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted;

(b) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.

2. The information referred to in paragraph 1 shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated in accordance with the procedures provided for in Article 34 shall normally forward the information.

Article 23

1. By way of derogation from Article 22(1), Member States may, in the case of the persons referred to in Article 2(1)(3)(a) and (b), designate an appropriate self-regulatory body of the profession concerned as the authority to be informed in the first instance in place of the FIU. Without prejudice to paragraph 2, the designated self-regulatory body shall in such cases forward the information to the FIU promptly and unfiltered.

2. Member States shall not be obliged to apply the obligations laid down in Article 22(1) to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 24

1. Member States shall require the institutions and persons covered by this Directive to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 22(1)(a). In conformity with the legislation of the Member States, instructions may be given not to carry out the transaction.

2. Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the institutions and persons concerned shall inform the FIU immediately afterwards.

Article 25

1. Member States shall ensure that if, in the course of inspections carried out in the institutions and persons covered by this Directive by the competent authorities referred to in Article 37, or in any other way, those authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 26

The disclosure in good faith as foreseen in Articles 22(1) and 23 by an institution or person covered by this Directive or by an employee or director of such an institution or person of the information referred to in Articles 22 and 23 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the institution or person or its directors or employees in liability of any kind.

Article 27

Member States shall take all appropriate measures in order to protect employees of the institutions or persons covered by this Directive who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to threats or hostile action.

SECTION 2

Prohibition of disclosure

Article 28

1. The institutions and persons covered by this Directive and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 22 and 23 or that a money laundering or terrorist financing investigation is being or may be carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities referred to in Article 37, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries provided that they meet the conditions laid down in Article 11(1), belonging to the same group as defined by Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate[1].

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between persons referred to in Article 2(1)(3)(a) and (b) from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not,

1 OJ L 35, 11.2.2003, p. 1.

within the same legal person or a network. For the purposes of this Article, a 'network' means the larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. For institutions or persons referred to in Article 2(1)(1), (2) and (3)(a) and (b) in cases related to the same customer and the same transaction involving two or more institutions or persons, the prohibition laid down in paragraph 1 shall not prevent disclosure between the relevant institutions or persons provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged shall be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

6. Where the persons referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute a disclosure within the meaning of the paragraph 1.

7. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 3, 4 or 5.

Article 29

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the disclosure between institutions and persons covered by this Directive and institutions and persons from the third country concerned.

CHAPTER IV

RECORD KEEPING AND STATISTICAL DATA

Article 30

Member States shall require the institutions and persons covered by this Directive to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law:

(a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended;

(b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following the carrying-out of the transactions or the end of the business relationship.

Article 31

1. Member States shall require the credit and financial institutions covered by this Directive to apply, where applicable, in their branches and majority-owned subsidiaries located in third countries measures at least equivalent to those laid down in this Directive with regard to customer due diligence and record keeping.

Where the legislation of the third country does not permit application of such equivalent measures, the Member States shall require the credit and financial institutions concerned to inform

the competent authorities of the relevant home Member State accordingly.

2. Member States and the Commission shall inform each other of cases where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1 and coordinated action could be taken to pursue a solution.

3. Member States shall require that, where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1, credit or financial institutions take additional measures to effectively handle the risk of money laundering or terrorist financing.

Article 32

Member States shall require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

Article 33

1. Member States shall ensure that they are able to review he effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.

2. Such statistics shall as a minimum cover the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and indicate on an annual basis the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and how much property has been frozen, seized or confiscated.

3. Member States shall ensure that a consolidated review of these statistical reports is published.

CHAPTER V

ENFORCEMENT MEASURES

SECTION 1

Internal procedures, training and feedback

Article 34

1. Member States shall require that the institutions and persons covered by this Directive establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

2. Member States shall require that credit and financial institutions covered by this Directive communicate relevant policies and procedures where applicable to branches and majority owned subsidiaries in third countries.

Article 35

1. Member States shall require that the institutions and persons covered by this Directive take appropriate measures so hat their relevant employees are aware of the provisions in force on the basis of this Directive. These measures shall include participation of their relevant employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

Where a natural person falling within any of the categories listed in Article 2(1)(3) performs his professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that the institutions and persons covered by this Directive have access to up-to-date information on the practices of money launderers and terrorist financers and on indications leading to the recognition of suspicious transactions.

3. Member States shall ensure that, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

SECTION 2

Supervision

Article 36

1. Member States shall provide that currency exchange offices and trust and company service providers shall be licensed or registered and casinos be licensed in order to operate their business legally. Without prejudice to future Community legislation, Member States shall provide that money transmission or remittance offices shall be licensed or registered in order to operate their business legally.

2. Member States shall require competent authorities to refuse licensing or registration of the entities referred to in paragraph 1 if they are not satisfied that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons.

Article 37

1. Member States shall require the competent authorities at least to effectively monitor and to take the necessary measures with a view to ensuring compliance with the requirements of this Directive by all the institutions and persons covered by this Directive.

2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate resources to perform their functions.

3. In the case of credit and financial institutions and casinos, competent authorities shall have enhanced supervisory powers, notably the possibility to conduct on-site inspections.

4. In the case of the natural and legal persons referred to in Article 2(1)(3)(a) to (e), Member States may allow the functions referred to in paragraph 1 to be performed on a risk-sensitive basis.

5. In the case of the persons referred to in Article 2(1)(3)(a)and (b), Member States may allow the functions referred to in paragraph 1 to be performed by self-regulatory bodies, provided that they comply with paragraph 2.

SECTION 3

Cooperation

Article 38

The Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community.

SECTION 4

Penalties

Article 39

1. Member States shall ensure that natural and legal persons covered by this Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The penalties must be effective, proportionate and dissuasive.

2. Without prejudice to the right of Member States to impose criminal penalties, Member States shall ensure, inconformity with their national law, that the appropriate administrative measures can be taken or administrative sanctions can be imposed against credit and financial institutions for infringements of the national provisions adopted pursuant to this Directive. Member States shall ensure that these measures or sanctions are effective, proportionate and dissuasive.

3. In the case of legal persons, Member States shall ensure that at least they can be held liable for infringements referred to in paragraph 1 which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person, or

(c) an authority to exercise control within the legal person.

4. In addition to the cases already provided for in paragraph3, Member States shall ensure that legal persons can beheld liable where the lack of supervision or control by a person referred to in paragraph 3 has made possible the commission of the infringements referred to in paragraph 1 for the benefit of a legal person by a person under its authority.

CHAPTER VI

IMPLEMENTING MEASURES

Article 40

1. In order to take account of technical developments in the fight against money laundering or terrorist financing and to ensure uniform implementation of this Directive, the Commission may, in

accordance with the procedure referred to in Article 41(2), adopt the following implementing measures:

(a) clarification of the technical aspects of the definitions in Article 3(2)(a) and (d), (6), (7), (8), (9) and (10);

(b) establishment of technical criteria for assessing whether situations represent a low risk of money laundering or terrorist financing as referred to in Article 11(2) and (5);

(c) establishment of technical criteria for assessing whether situations represent a high risk of money laundering or terrorist financing as referred to in Article 13;

(d) establishment of technical criteria for assessing whether, in accordance with Article 2(2), it is justified not to apply this Directive to certain legal or natural persons carrying out a financial activity on an occasional or very limited basis.

2. In any event, the Commission shall adopt the first implementing measures to give effect to paragraphs 1(b) and 1(d) by15 June 2006.

3. The Commission shall, in accordance with the procedure referred to in Article 41(2), adapt the amounts referred to in Articles 2(1)(3)(e), 7(b), 10(1) and 11(5)(a) and (d) taking into account Community legislation, economic developments and changes in international standards.

4. Where the Commission finds that a third country does not meet the conditions laid down in Article 11(1) or (2),Article 28(3), (4) or (5), or in the measures established in accordance with paragraph 1(b) of this Article or in Article 16(1)(b), or that the legislation of that third country does not permit application of the measures required under the first subparagraph of Article 31(1), it shall adopt a decision so stating in accordance with the procedure referred to in Article 41(2).

Article 41

1. The Commission shall be assisted by a Committee on the Prevention of Money Laundering and Terrorist Financing, hereinafter 'the Committee'.

2. Where reference is made to this paragraph, Articles 5 and7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof and provided that the implementing measures adopted in accordance with this procedure do not modify the essential provisions of this Directive. The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its Rules of Procedure.

4. Without prejudice to the implementing measures already adopted, the implementation of the provisions of this Directive concerning the adoption of technical rules and decisions in accordance with the procedure referred to in paragraph 2 shall be suspended four years after the entry into force of this Directive. On a proposal from the Commission, the European Parliament and the Council may renew the provisions concerned in accordance with the procedure laid down in Article 251 of the Treaty and, to that end, shall review them prior to the expiry of the four-year period.

CHAPTER VII

FINAL PROVISIONS

Article 42

By 15 December 2009, and at least at three-yearly intervals thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and the Council. For the first such report, the Commission shall include a specific examination of the treatment of lawyers and other independent legal professionals.

Article 43

By 15 December 2010, the Commission shall present a report to the European Parliament and to the Council on the threshold percentages in Article 3(6), paying particular attention to the possible expediency and consequences of a reduction of the percentage in points (a)(i), (b)(i) and (b)(iii) of Article 3(6) from25 % to 20 %. On the basis of the report the Commission may submit a proposal for amendments to this Directive.

Article 44

Directive 91/308/EEC is hereby repealed. References made to the repealed Directive shall be construed as being made to this Directive and should be read in accordance with the correlation table set out in the Annex.

Article 45

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 15 December 2007. They shall forthwith communicate to the Commission the text of those provisions together with a table showing how the provisions of this Directive correspond to the national provisions adopted. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 46

This Directive shall enter into force on the 20th day after its publication in the Official Journal of the European Union.

Article 47

This Directive is addressed to the Member States.

Done at Strasbourg, 26 October 2005.

For the European Parliament	*For the Council*
The President	*The President*
J. BORRELL FONTELLES	D. ALEXANDER

ANNEX

CORRELATION TABLE

This Directive	**Directive 91/308/EEC**
Article 1(1)	Article 2
Article 1(2)	Article 1(C)
Article 1(2)(a)	Article 1(C) first point
Article 1(2)(b)	Article 1(C) second point
Article 1(2)(c)	Article 1(C) third point
Article 1(2)(d)	Article 1(C) fourth point
Article 1(3)	Article 1(C), third paragraph
Article 1(4)	
Article 1(5)	Article 1(C), second paragraph
Article 2(1)(1)	Article 2a(1)
Article 2(1)(2)	Article 2a(2)
Article 2(1)(3)(a), (b) and (d) to (f)	Article 2a(3) to (7)
Article 2(1)(3)(c)	
Article 2(2)	
Article 3(1)	Article 1(A)
Article 3(2)(a)	Article 1(B)(1)
Article 3(2)(b)	Article 1(B)(2)
Article 3(2)(c)	Article 1(B)(3)
Article 3(2)(d)	Article 1(B)(4)
Article 3(2)(e)	
Article 3(2)(f)	Article 1(B), second paragraph

Article 3(3)	Article 1(D)
Article 3(4)	Article 1(E), first paragraph
Article 3(5)	Article 1(E), second paragraph
Article 3(5)(a)	
Article 3(5)(b)	Article 1(E), first indent
Article 3(5)(c)	Article 1(E), second indent
Article 3(5)(d)	Article 1(E), third indent
Article 3(5)(e)	Article 1(E), fourth indent
Article 3(5)(f)	Article 1(E), fifth indent, and third paragraph
Article 3(6)	
Article 3(7)	
Article 3(8)	
Article 3(9)	
Article 3(10)	
Article 4	Article 12
Article 5	article 15
Article 6	
Article 7(a)	Article 3(1)
Article 7(b)	Article 3(2)
Article 7(c)	Article 3(8)
Article 7(d)	Article 3(7)
Article 8(1)(a)	Article 3(1)
Article 8(1)(b) to (d)	
Article 8(2)	
Article 9(1)	Article 3(1)
Article 9(2) to (6)	
Article 10	Article 3(5) and (6

Article 11(1)	Article 3(9)
Article 11(2)	
Article 11(3) and (4)	
Article 11(5)(a)	Article 3(3)
Article 11(5)(b)	Article 3(4)
Article 11(5)(c)	Article 3(4)
Article 11(5)(d)	
Article 12	
Article 13(1) and (2)	Article 3(10) and (11)
Article 13(3) to (5)	
Article 13(6)	Article 5
Article 14	
Article 15	
Article 16	
Article 17	
Article 18	
Article 19	
Article 20	Article 5
Article 21	
Article 22	Article 6(1) and (2)
Article 23	Article 6(3)
Article 24	Article 7
Article 25	Article 10
Article 26	Article 9
Article 27	
Article 28(1)	Article 8(1)
Article 28(2) to (7)	

Article 29	
Article 30(a)	Article 4, first indent
Article 30(b)	Article 4, second indent
Article 31	
Article 32	
Article 33	
Article 34(1)	Article 11(1) (a
Article 34(2)	
Article 35(1), first paragraph	Article 11(1)(b), first sentence
Article 35(1), second paragraph	Article 11(1)(b) second sentence
Article 35(1), third paragraph	Article 11(1), second paragraph
Article 35(2)	
Article 35(3)	
Article 36	
Article 37	
Article 38	
Article 39(1)	Article 14
Article 39(2) to (4)	
Article 40	
Article 41	
Article 42	Article 17
Article 43	
Article 44	
Article 45	Article 16
Article 46	Article 16

Association of Certified Anti-Money Laundering Specialists®

ACAMS®

BRICKELL BAYVIEW CENTER
80 SOUTHWEST 8TH STREET, SUITE 2350
MIAMI, FLORIDA 33130 USA

TELEPHONES: +1.305.373.0020 OR
+1.866.459.CAMS IN THE UNITED STATES
FAX: +1.305.373.7788 OR
+1.305.373.5229
EMAIL: INFO@ACAMS.ORG

ACAMS.ORG
ACAMS.ORG/ESPANOL