



UNODC

United Nations Office on Drugs and Crime

GPML

Global Programme against Money Laundering,
Proceeds of Crime and the Financing of Terrorism

**AN OVERVIEW OF THE UN CONVENTIONS AND OTHER
INTERNATIONAL STANDARDS CONCERNING ANTI-MONEY
LAUNDERING AND COUNTERING THE FINANCING OF
TERRORISM**

Vienna, January 2013

1	DEFINITIONS - FINANCIAL	8
1.1.1	<i>FATF Recommendations</i>	8
1.1.2	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	12
1.1.3	<i>Directive 2005/60/EC of the European Parliament and of the Council of 25 October 2005 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)</i>	12
2	CUSTOMER IDENTIFICATION	15
2.1.1	<i>FATF Recommendations</i>	15
2.1.2	<i>Basel Committee on Banking Supervision - Customer due diligence</i>	24
2.1.3	<i>Wolfsberg AML Principles</i>	29
2.1.4	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	30
2.1.5	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)</i>	31
3	RECORD KEEPING	36
3.1.1	<i>FATF Recommendations</i>	36
3.1.2	<i>Basel Committee on Banking Supervision - Customer due diligence</i>	36
3.1.3	<i>Wolfsberg AML Principles</i>	36
3.1.4	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	36
3.1.5	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)</i>	37
4	REPORTING	38
4.1.1	<i>FATF Recommendations</i>	38
4.1.2	<i>Wolfsberg AML Principles</i>	38
4.1.3	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	39
4.1.4	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)</i>	39
5	FAILING TO REPORT AND TIPPING OFF	40
5.1	SPECIAL ATTENTION	40
5.1.1	<i>FATF Recommendations</i>	40
5.1.2	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing</i>	40
5.2	NO TIPPING OFF	41
5.2.1	<i>FATF Recommendations</i>	41

5.2.2	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	41
5.2.3	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist</i>	41
5.3	SANCTIONS OR PENALTIES	42
5.3.1	<i>FATF Recommendations</i>	42
5.3.2	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)</i>	42
6	INTERNAL REPORTING SYSTEM/TRAINING/EDUCATION	43
6.1.1	<i>FATF Recommendations</i>	43
6.1.2	<i>2000 UN Convention against Transnational Organized Crime</i>	43
6.1.3	<i>Basel Committee on Banking Supervision - Customer due diligence</i>	44
6.1.4	<i>Wolfsberg AML Principles</i>	45
6.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	45
6.1.6	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist</i>	45
7	SUPERVISION	47
7.1.1	<i>FATF Recommendations</i>	47
7.1.2	<i>Basel Committee on Banking Supervision - Customer due diligence</i>	48
7.1.3	<i>2000 UN Convention against Transnational Organized Crime</i>	51
7.1.4	<i>2003 UN Convention against Corruption</i>	51
7.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	51
7.1.6	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)</i>	51
8	DEFINITIONS – PENAL	53
8.1.1	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances</i>	53
8.1.2	<i>2000 UN Convention against Transnational Organized Crime</i>	53
8.1.3	<i>2003 UN Convention against Corruption</i>	53
8.1.4	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	54
9	MONEY LAUNDERING OFFENCES	55
9.1.1	<i>FATF Recommendations</i>	55
9.1.2	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances</i>	56
9.1.3	<i>2000 UN Convention against Transnational Organized Crime</i>	57
9.1.4	<i>2003 UN Convention against Corruption</i>	58
9.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	59

9.1.6	<i>Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime</i>	60
10	PROVISIONAL MEASURES AND CONFISCATION	61
10.1.1	<i>FATF Recommendations</i>	61
10.1.2	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances</i>	62
10.1.3	<i>2000 UN Convention against Transnational Organized Crime</i>	62
10.1.4	<i>2003 UN Convention against Corruption</i>	63
10.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	63
10.1.6	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)</i>	64
10.1.7	<i>Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime</i>	64
11	BEARER SHARES, TRUSTS AND CORPORATE CRIMINAL LIABILITY	66
11.1.1	<i>FATF Recommendations</i>	66
11.1.2	<i>2000 UN Convention against Transnational Organized Crime</i>	69
11.1.3	<i>2003 UN Convention against Corruption</i>	69
11.1.4	<i>Basel Committee on Banking Supervision - Customer due diligence</i>	70
11.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	70
11.1.6	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)</i>	70
11.2	SHELL BANKS	71
11.2.1	<i>FATF Recommendations</i>	71
11.2.2	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist</i>	71
12	NATIONAL CO-OPERATION	72
12.1.1	<i>FATF Recommendations</i>	72
12.1.2	<i>2000 UN Convention against Transnational Organized Crime</i>	72
12.1.3	<i>2003 UN Convention against Corruption</i>	72
12.1.4	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)</i>	73
13	INTERNATIONAL CO-OPERATION	74
13.1	MUTUAL LEGAL ASSISTANCE – LAW ENFORCEMENT CO-OPERATION	74
13.1.1	<i>FATF Recommendations</i>	74
13.1.2	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances</i>	76
13.1.3	<i>2000 UN Convention against Transnational Organized Crime</i>	78
13.1.4	<i>2003 UN Convention against Corruption</i>	82

13.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	85
13.1.6	<i>The 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU</i>	89
13.1.7	<i>Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime</i>	90
13.1.8	<i>The protocol to the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU</i>	91
13.2	ASSET RECOVERY	92
13.2.1	<i>FATF Recommendations</i>	92
13.2.2	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances</i>	93
13.2.3	<i>2000 UN Convention against Transnational Organized Crime</i>	93
13.2.4	<i>2003 UN Convention against Corruption</i>	94
13.2.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	97
13.3	JURISDICTION AND EXTRADITION.....	101
13.3.1	<i>FATF Recommendations</i>	101
13.3.2	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances</i>	101
13.3.3	<i>2000 UN Convention against Transnational Organized Crime</i>	102
13.3.4	<i>2003 UN Convention against Corruption</i>	104
13.3.5	<i>Council of the EU Framework Decision on the European arrest warrant and the surrender procedures between Member States</i>	106
13.4	RATIFICATION AND IMPLEMENTATION	107
13.4.1	<i>FATF Recommendations</i>	107
13.4.2	<i>1998 UN Political Declaration and Action Plan against Money Laundering</i>	107
13.4.3	<i>2001 Conference of the G8 Ministers of Justice and Interior</i>	108
13.4.4	<i>Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime</i>	108
13.4.5	<i>2001 Joint ECOFIN/JHA meeting</i>	108
14	FINANCIAL INTELLIGENCE UNITS (FIU).....	109
14.1.1	<i>FATF Recommendations</i>	109
14.1.2	<i>Egmont – Statement of purpose</i>	110
14.1.3	<i>Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases</i>	110
14.1.4	<i>2003 UN Convention against Corruption</i>	111
14.1.5	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism</i>	111
14.1.6	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)</i>	112

14.1.7	<i>Council of the EU Decision concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.....</i>	112
14.1.8	<i>2001 Joint ECOFIN/JHA meeting.....</i>	114
15	OTHER ISSUES.....	115
15.1	CONTROLLED DELIVERY.....	115
15.1.1	<i>FATF Recommendations.....</i>	115
15.1.2	<i>1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances.....</i>	116
15.1.3	<i>2000 UN Convention against Transnational Organized Crime.....</i>	116
15.1.4	<i>2003 UN Convention against Corruption.....</i>	117
15.1.5	<i>The 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU.....</i>	117
15.2	CROSS-BORDER TRANSPORTATION OF CASH.....	117
15.2.1	<i>FATF Recommendations.....</i>	117
15.2.2	<i>2000 UN Convention against Transnational Organized Crime.....</i>	119
15.2.3	<i>2003 UN Convention against Corruption.....</i>	119
15.2.4	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism.....</i>	119
15.3	IMMUNITY CLAUSE.....	120
15.3.1	<i>FATF Recommendations.....</i>	120
15.3.2	<i>Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)..</i>	120
15.4	NEW TECHNIQUES.....	120
15.4.1	<i>FATF Recommendations.....</i>	120
15.4.2	<i>2000 UN Convention against Transnational Organized Crime.....</i>	120
15.4.3	<i>2003 UN Convention against Corruption.....</i>	121
15.4.4	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism.....</i>	121
15.5	TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION.....	121
15.5.1	<i>FATF Recommendations.....</i>	121
16	TERRORIST FINANCING.....	125
16.1.1	<i>FATF Recommendations on Terrorist Financing.....</i>	125
16.1.2	<i>1999 UN International Convention for the Suppression of the Financing of Terrorism.....</i>	132
16.1.3	<i>UN Resolution 1373.....</i>	137
16.1.4	<i>2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism.....</i>	138
16.1.5	<i>Wolfsberg Statement on the suppression of the financing of terrorism.....</i>	138
16.1.6	<i>Council of the EU Framework Decision on combating terrorism.....</i>	139

1 DEFINITIONS - FINANCIAL

1.1.1 FATF Recommendations¹

Definitions

Country All references in the FATF Recommendations to country or countries apply equally to territories or jurisdictions.

Criminal activity Criminal activity refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.

Designated nonfinancial businesses and professions means:

- a) Casinos.²
- 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 AML/CFT measures.
- 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 or performing the equivalent function for another form of legal arrangement;
 - acting as (or arranging for another person to act as) a nominee shareholder for another person.

Enforceable means Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.

Financial institutions means any natural or legal person 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.³
2. Lending.⁴
3. Financial leasing.⁵
4. Money or value transfer services.⁶
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, certificates of deposit, derivatives etc.);
 - (b) foreign exchange;
 - (c) exchange, interest rate and index instruments;
 - (d) transferable securities;
 - (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.

¹ FATF Recommendations refers to Recommendations issued by FATF in February 2012

² References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

³ This also captures private banking.

⁴ This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

⁵ This does not extend to financial leasing arrangements in relation to consumer products.

⁶ 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 Interpretive Note to Recommendation 16.

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.⁷

13. Money and currency changing.

Fundamental principles of domestic law refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.

Funds refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.

Funds or other assets means any assets, including, but not limited to, financial assets, economic resources, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

Law Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.

Money laundering offence References (except in Recommendation 3) to a money laundering offence refer not only to the primary offence or offences, but also to ancillary offences.

Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.

Reasonable measures means appropriate measures which are commensurate with the money laundering or terrorist financing risks.

Risk refers to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.

Satisfied 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.

Self-regulatory body (SRB) is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession.

Should For the purposes of assessing compliance with the FATF Recommendations, the word should has the same meaning as must.

Terrorist financing offence References (except in Recommendation 4) to a terrorist financing offence refer not only to the primary offence or offences, but also to ancillary offences.

Recommendation 22

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) 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 following activities:
 - 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;

⁷ This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

- 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 or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

Interpretative note to Recommendation 22

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.
2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

Recommendation 23

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial 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 paragraph (d) of Recommendation 22. 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 in paragraph (e) of Recommendation 22.

Interpretative note to Recommendation 23

1. Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
2. It is for each country 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.
3. 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 cooperation between these organisations and the FIU.
4. 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.

Interpretative note to Recommendations 22 and 23

The designated thresholds for transactions are as follows:

- Casinos (under Recommendation 22) - USD/EUR 3,000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - 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.

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means 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 enforceable means covering the underlying activities.

Recommendation 1

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of riskbased measures throughout the FATF Recommendations. Where countries identify higher

risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions. Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

Interpretative Note to Recommendation 1

The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

3. Countries⁸ should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to:

(i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures;

(ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and

(iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs.

Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on

the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

4. Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

5. Countries may decide to allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 3. Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified customer due diligence (CDD) measures, provided that the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 7 below, are met.

6. Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:

(a) there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

(b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.

⁸ Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

7. Supervisors (or SRBs for relevant DNFBBs sectors) should ensure that financial institutions and DNFBBs are effectively implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBBs, and take the result of this review into consideration.

8. Financial institutions and DNFBBs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBBs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

9. Financial institutions and DNFBBs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBB). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.

10. Where higher risks are identified financial institutions and DNFBBs should be required to take enhanced measures to manage and mitigate the risks.

11. Where lower risks are identified, countries may allow financial institutions and DNFBBs to take simplified measures to manage and mitigate those risks.

12. When assessing risk, financial institutions and DNFBBs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBBs may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

1.1.2 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

1 Each Party shall adopt such legislative and other measures as may be necessary to institute a comprehensive domestic regulatory and supervisory or monitoring regime to prevent money laundering and shall take due account of applicable international standards, including in particular the recommendations adopted by the Financial Action Task Force on Money Laundering (FATF).

1.1.3 Directive 2005/60/EC of the European Parliament and of the Council of 25 October 2005 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)

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 Decision 2002/475/JHA of 13 June 2002 on combating terrorism.
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;
 - (3) the following legal or natural persons acting in the exercise of 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, 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 points 14 and 15 of Annex I to Directive 2006/48/EC, including the activities of currency exchange offices (bureaux de change);
 - (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, 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;
 - (d) a collective investment undertaking marketing its units or shares;
 - (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, 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);

(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;

(e) corruption;

(f) all offences which are punishable by deprivation of liberty 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;

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.

ANNEX

LIST OF ACTIVITIES SUBJECT TO MUTUAL RECOGNITION

1. Acceptance of deposits and other repayable funds

2. Lending(1)

3. Financial leasing

4. Money transmission services

5. Issuing and administering means of payment (e.g. credit cards, travellers' cheques and bankers' drafts)

6. Guarantees and commitments

7. Trading for own account or for account of customers in:

(a) money market instruments (cheques, bills, certificates of deposit, etc.)

(b) foreign exchange;

(c) financial futures and options;

(d) exchange and interest-rate instruments;

(e) transferable securities

8. Participation in securities issues and the provision of services related to such issues

9. Advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings

10. Money broking

11. Portfolio management and advice

12. Safekeeping and administration of securities

13. Credit reference services

14. Safe custody services

(1) Including, inter alia:

- consumer credit,

- mortgage credit,

- factoring, with or without recourse,

- financing of commercial transactions (including forfeiting).

2 CUSTOMER IDENTIFICATION

2.1.1 FATF Recommendations

Definitions

Accounts References to “accounts” should be read as including other similar business relationships between financial institutions and their customers.

Accurate is used to describe information that has been verified for accuracy.

Agent For the purposes of Recommendations 14 and 16, agent means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.

Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.

Beneficial owner refers to the natural person(s) who ultimately⁹ owns or controls a customer¹⁰ and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Beneficiary The meaning of the term beneficiary in the FATF Recommendations depends on the context:

- In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally coextensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.
- In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendations 8 and 16.

Beneficiary Financial Institution refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.

Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

Cross-border Wire Transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

Domestic Wire Transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of wire transfer that takes place entirely within the borders of the European Economic Area (EEA).¹¹

Identification data refers to reliable, independent source documents, data or information.

Intermediary financial institution refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation;

⁹ Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

¹⁰ This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

¹¹ An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Cooperation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

Legal arrangements Legal arrangements refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.

Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Money or value transfer service (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen.

Ordering financial institution refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for an wire transfer on behalf of the originator.

Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

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): Foreign PEPs are individuals who are or have been entrusted with prominent public functions by 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 party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Qualifying wire transfers means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.

Required is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the required originator information. Subparagraphs 6(d) and 6(e) set out the required beneficiary information.

Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).

Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

Third parties means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.¹²

Recommendation 10

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when:

- (i) establishing business relations;

¹² It is understood that the settlement of wire transfers may happen under a net settlement arrangement.

This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).

- (ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- (iii) there is a suspicion of money laundering or terrorist financing; or
- (iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The 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.
- (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 understanding the ownership and control structure of the customer.
- (c) Understanding and, as appropriate, 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 be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1. Financial institutions should be required to 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 and terrorist financing 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 the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to 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, although 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.

Interpretative Note to Recommendation 10

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 identity¹³ of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and
- (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

2. Recommendation 21 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 CDD 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.

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements¹⁴, financial institutions should be required to identify and verify the customer, and understand the nature of its business, and its

¹³ Reliable, independent source documents, data or information will hereafter be referred to as "identification data."

¹⁴ In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee

ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

(a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

(i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

(ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

(iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures¹⁵ to verify the identity of such persons, through the following information:

(i) For legal persons¹⁶:

(i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest¹⁷ in a legal person; and

(i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries¹⁸, and any other natural person exercising ultimate effective control over the trust (including through a

chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

¹⁵ In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

¹⁶ Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

¹⁷ A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

¹⁸ For beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

10. The CDD measures set out in Recommendation 10 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.

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) 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.

12. 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 the expected norms for that type of relationship.

13. Financial institutions should be required to apply CDD measures to existing customers¹⁹ on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

32 Existing customers as at the date that the national requirements are brought into force.

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:²⁰

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties.

¹⁹ Existing customers as at the date that the national requirements are brought into force.

²⁰ Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option 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.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures

should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

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

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

23. Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

Recommendation 12

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

- (a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- (b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- (c) take reasonable measures to establish the source of wealth and source of funds; and
- (d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Interpretative Note to Recommendation 12

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

- a) inform senior management before the payout of the policy proceeds; and
- b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

Recommendation 13

Financial institutions should be required, in relation to cross-border and other similar relationships, in addition to performing normal customer due diligence measures, 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, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- (b) assess the respondent institution's AML/CFT controls;
- (c) obtain approval from senior management before establishing new correspondent relationships;
- (d) clearly understand the respective responsibilities of each institution; and
- (e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

Interpretative Note to Recommendation 13

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Recommendation 14

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

Interpretative Note to Recommendation 14

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

Recommendation 16

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

Interpretative Note to Recommendation 16

1. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

- (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;
- (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and
- (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

2. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

3. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers, including serial payments, and cover payments.

4. Recommendation 16 is not intended to cover the following types of payments:

- (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction.

However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

- (b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

5. Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

(a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

(b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

6. Information accompanying all qualifying wire transfers should always contain:

(a) the name of the originator;

(b) the originator account number where such an account is used to process the transaction;

(c) the originator's address, or national identity number, or customer identification number²¹, or date and place of birth;

(d) the name of the beneficiary; and

(e) the beneficiary account number where such an account is used to process the transaction.

7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

8. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

9. Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

10. The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

11. The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.

12. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.

13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

14. The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.

15. For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

16. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

17. An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

20. For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

²¹ The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

22. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

(a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Recommendation 17

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures 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 measures set out in Recommendation 10.

(b) 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.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

Interpretative Note to Recommendation 17

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.

2. For the purposes of Recommendation 17, the term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

2.1.2 Basel Committee on Banking Supervision - Customer due diligence

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”. 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. 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.

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.

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.

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 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.

2.2.1 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.

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:

- 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 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 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 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. 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.

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 non-face-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.

47. Even though the same documentation can be provided by face-to-face and non-face-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.

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

- banks should apply equally effective customer identification procedures for non-face-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 “non-cooperative” 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 through 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-money-laundering 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. 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.

2.1.3 Wolfsberg AML Principles

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 fulfillment 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.

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.

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 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 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.

2.2 High-risk countries

The bank will apply heightened scrutiny to clients and beneficial owners resident in and funds sourced from countries identified by credible sources as having inadequate anti-money-laundering standards or representing high-risk for crime and corruption.

2.3 Offshore jurisdictions

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

2.4 High-risk activities

Clients and beneficial owners whose source of wealth emanates from activities known to be susceptible to money laundering will be subject to heightened scrutiny.

2.5 Public officials

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 require heightened scrutiny.

3 Updating client files

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.

2.1.4 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

2 In that respect, each Party shall adopt, in particular, such legislative and other measures as may be necessary to:

- a) require legal and natural persons which engage in activities which are particularly likely to be used for money laundering purposes, and as far as these activities are concerned, to:
 - i) identify and verify the identity of their customers and, where applicable, their ultimate beneficial owners, and to conduct ongoing due diligence on the business relationship, while taking into account a risk based approach;

2.1.5 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)

Article 3

(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;

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 sub-paragraph 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.

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.

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, the European Supervisory Authority (European Banking Authority) (hereinafter 'EBA'), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council (1), the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (hereinafter 'EIOPA'), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council (2), and the European Supervisory Authority (European Securities and Markets Authority) (hereinafter 'ESMA'), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council (3) (collectively, the 'ESA') to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010, 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 more than 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;

(d) electronic money, as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions (1) where, if it is not possible to recharge, the maximum amount stored electronically in the device is no more than EUR 250, or where, if it is possible to recharge, 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 upon the electronic money holder's request in accordance with Article 11 of Directive 2009/110/EC. As regards national payment transactions, Member States or their competent authorities may increase the amount of EUR 250 referred to in this point to a ceiling of EUR 500.

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).

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.

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 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 payment institutions as defined in Article 4(4) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (1), which mainly provide the payment service listed in point 6 of the Annex to that Directive, including natural and legal persons benefiting from a waiver under Article 26 of that Directive, and meeting the requirements laid down in Articles 16 and 18 of this Directive, 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 referred to in Article 3(2)(a) and payment institutions as defined in Article 4(4) of Directive 2007/64/EC, which mainly provide the payment service listed in point 6 of the Annex to that Directive, 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 of this Directive, 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 of this Directive, 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. The Member States shall inform each other, the ESA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010, 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.

3 RECORD KEEPING

3.1.1 FATF Recommendations

Definitions

Competent authorities refers to all public authorities²² with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.

Recommendation 11

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and 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 be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction. Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures. The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

3.1.2 Basel Committee on Banking Supervision - Customer due diligence

26. Banks should develop “clear standards on what records must be kept on customer identification and individual transactions and their retention period”. 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.

3.1.3 Wolfsberg AML Principles

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.

3.1.4 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

2 In that respect, each Party shall adopt, in particular, such legislative and other measures as may be necessary to:

a) require legal and natural persons which engage in activities which are particularly likely to be used for money laundering purposes, and as far as these activities are concerned, to:

iii) take supporting measures, such as record keeping on customer identification and transactions, training of personnel and the establishment of internal policies and procedures, and if appropriate, adapted to their size and nature of business;

²² This includes financial supervisors established as independent non-governmental authorities with statutory powers.

3.1.5 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)

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.

4 REPORTING

4.1.1 FATF Recommendations

Recommendation 20

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, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

Interpretative Note to Recommendation 20

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.
2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organizations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.
3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.
4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called “indirect reporting”), is not acceptable.

4.1.2 Wolfsberg AML Principles

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.

4.1.3 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

2 In that respect, each Party shall adopt, in particular, such legislative and other measures as may be necessary to:
a require legal and natural persons which engage in activities which are particularly likely to be used for money laundering purposes, and as far as these activities are concerned, to:

ii report suspicions on money laundering subject to safeguard;

4.1.4 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)

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.

5 FAILING TO REPORT AND TIPPING OFF

5.1 Special attention

5.1.1 FATF Recommendations

Recommendation 19

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

Interpretative note to Recommendation 19

The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.

2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

- (a) Requiring financial institutions to apply specific elements of enhanced due diligence.
- (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.
- (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
- (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.
- (e) Limiting business relationships or financial transactions with the identified country or persons in that country.
- (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.
- (g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.
- (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.
- (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

5.1.2 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Article 13

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.

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.

5.2 No tipping off

5.2.1 FATF 40 Recommendations

Recommendation 21

Financial institutions, their directors, officers and employees should be:

(a) ...

(b) prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

5.2.2 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

2 In that respect, each Party shall adopt, in particular, such legislative and other measures as may be necessary to:

b prohibit, as appropriate, the persons referred to in sub-paragraph a from disclosing the fact that a suspicious transaction report or related information has been transmitted or that a money laundering investigation is being or may be carried out;

5.2.3 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist

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.

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, 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, the ESA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 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.

5.3 Sanctions or penalties

5.3.1 FATF Recommendations

Recommendation 35

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

5.3.2 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)

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, in conformity 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 paragraph

3, Member States shall ensure that legal persons can be held 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.

6 INTERNAL REPORTING SYSTEM/TRAINING/EDUCATION

6.1.1 FATF Recommendations

Definitions

Financial group means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

Recommendation 18

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement groupwide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

Interpretative note to Recommendation 18

Financial institutions' programmes against money laundering and terrorist financing 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; and
- (c) an independent audit function to test the system.

2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

3. Compliance management arrangements should include the appointment of a compliance officer at the management level.

4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place.

5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including, as appropriate, requesting the financial group to close down its operations in the host country.

6.1.2 2000 UN Convention against Transnational Organized Crime

Article 29 - Training and technical assistance

1. Each State Party shall, to the extent necessary, initiate, develop or improve specific training programmes for its law enforcement personnel, including prosecutors, investigating magistrates and customs personnel, and other personnel charged with the prevention, detection and control of the offences covered by this Convention. Such programmes may include secondments and exchanges of staff. Such programmes shall deal, in particular and to the extent permitted by domestic law, with the following:

- (a) Methods used in the prevention, detection and control of the offences covered by this Convention;
- (b) Routes and techniques used by persons suspected of involvement in offences covered by this Convention, including in transit States, and appropriate countermeasures;
- (c) Monitoring of the movement of contraband;
- (d) Detection and monitoring of the movements of proceeds of crime, property, equipment or other instrumentalities and methods used for the transfer, concealment or disguise of such proceeds, property, equipment or other instrumentalities, as well as methods used in combating money-laundering and other financial crimes;

- (e) Collection of evidence;
- (f) Control techniques in free trade zones and free ports;
- (g) Modern law enforcement equipment and techniques, including electronic surveillance, controlled deliveries and undercover operations;
- (h) Methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology; and
- (i) Methods used in the protection of victims and witnesses.

2. States Parties shall assist one another in planning and implementing research and training programmes designed to share expertise in the areas referred to in paragraph 1 of this article and to that end shall also, when appropriate, use regional and international conferences and seminars to promote cooperation and to stimulate discussion on problems of mutual concern, including the special problems and needs of transit States.

3. States Parties shall promote training and technical assistance that will facilitate extradition and mutual legal assistance. Such training and technical assistance may include language training, secondments and exchanges between personnel in central authorities or agencies with relevant responsibilities.

4. In the case of existing bilateral and multilateral agreements or arrangements, States Parties shall strengthen, to the extent necessary, efforts to maximize operational and training activities within international and regional organizations and within other relevant bilateral and multilateral agreements or arrangements.

6.1.3 Basel Committee on Banking Supervision - Customer due diligence

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 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 well-versed 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.

6.1.4 Wolfsberg AML Principles

5 Monitoring

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.

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.

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.

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).

6.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

2 In that respect, each Party shall adopt, in particular, such legislative and other measures as may be necessary to: a require legal and natural persons which engage in activities which are particularly likely to be used for money laundering purposes, and as far as these activities are concerned, to:

iii take supporting measures, such as record keeping on customer identification and transactions, training of personnel and the establishment of internal policies and procedures, and if appropriate, adapted to their size and nature of business;

6.1.6 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist

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.

3. In order to ensure consistent harmonisation and to take account of technical developments in the fight against money laundering and terrorist financing, the ESA, taking into account the existing framework and cooperating, as appropriate, with other relevant Union bodies in that field, may develop draft regulatory technical standards in accordance with Article 56 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010 respectively, to specify the minimum content of the communication referred to in paragraph 2.

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

Article 35

1. Member States shall require that the institutions and persons covered by this Directive take appropriate measures so that 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 financiers 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.

7 SUPERVISION

7.1.1 FATF Recommendations

Definitions

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.

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions (“financial supervisors”²³) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These nonpublic bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

Recommendation 26

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors 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.

Countries should not approve the establishment, or continued operation, of shell banks.

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 and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes. Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

Interpretative Note to Recommendation 26

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.
2. Adopting a risk-based approach to supervising financial institutions’ AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group (or groups, when applicable for Core Principles institutions). The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor’s assessment of the institution/group’s risk profile, and on the money laundering and terrorist financing risks present in the country.
3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country’s established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.
4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.

²³ Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and autonomy to ensure freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Recommendation 27

Supervisors should have adequate powers to supervise or 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 authorized to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

Recommendation 28

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 AML/CFT 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; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

Interpretative Note to Recommendation 28

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.

2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.

3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.

4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

7.1.2 Basel Committee on Banking Supervision - Customer due diligence

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. 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.

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 group wide 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 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.

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 being used, intentionally or unintentionally, by criminal elements.

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 anti-money-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.

7.1.3 2000 UN Convention against Transnational Organized Crime

Article 7 - Measures to combat money-laundering

1. Each State Party:

(a) Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions;

3. In establishing a domestic regulatory and supervisory regime under the terms of this article, and without prejudice to any other article of this Convention, States Parties are called upon to use as a guideline the relevant initiatives of regional, interregional and multilateral organizations against money-laundering.

7.1.4 2003 UN Convention against Corruption

Article 14 - Measures to prevent money-laundering

1. Each State Party shall:

(a) Institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions, including natural or legal persons that provide formal or informal services for the transmission of money or value and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer and, where appropriate, beneficial owner identification, record-keeping and the reporting of suspicious transactions;

4. In establishing a domestic regulatory and supervisory regime under the terms of this article, and without prejudice to any other article of this Convention, States Parties are called upon to use as a guideline the relevant initiatives of regional, interregional and multilateral organizations against money-laundering.

7.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

2. In that respect, each Party shall adopt, in particular, such legislative and other measures as may be necessary to:

c. ensure that the persons referred to in sub-paragraph a are subject to effective systems for monitoring, and where applicable supervision, with a view to ensure their compliance with the requirements to combat money laundering, where appropriate on a risk sensitive basis.

7.1.6 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)

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 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. The Member States, the ESA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 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.

4. In order to ensure consistent harmonisation of this Article and to take account of technical developments in the fight against money laundering and terrorist financing, the ESA taking into account the existing framework and cooperating, as appropriate, with other relevant Union bodies in that field, may develop draft regulatory technical standards in accordance with Article 56 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 respectively to specify the type of additional measures referred to in paragraph 3 of this Article and the minimum action to be taken by credit and financial institutions where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1 of this Article.

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

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.

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.

8 DEFINITIONS – PENAL

8.1.1 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 1

(f) "Confiscation", which includes forfeiture where applicable, means the permanent deprivation of property by order of a court or other competent authority;

(l) "Freezing" or "seizure" means temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or a competent authority;

(p) "Proceeds" means any property derived from or obtained, directly or indirectly, through the commission of an offence established in accordance with article 3, paragraph 1;

(q) "Property" means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets;

8.1.2 2000 UN Convention against Transnational Organized Crime

Article 2 - Use of terms

For the purposes of this Convention:

(a) "Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

(b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

(c) "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure;

(d) "Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets;

(e) "Proceeds of crime" shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

(f) "Freezing" or "seizure" shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

(g) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

(h) "Predicate offence" shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 6 of this Convention;

8.1.3 2003 UN Convention against Corruption

Article 2- Use of terms

For the purposes of this Convention:

(d) "Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to or interest in such assets;

(e) "Proceeds of crime" shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

(f) "Freezing" or "seizure" shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

(g) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

(h) "Predicate offence" shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 23 of this Convention;

8.1.4 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 1 – Use of terms

For the purposes of this Convention:

a "proceeds" means any economic advantage, derived from or obtained, directly or indirectly, from criminal offences.

It may consist of any property as defined in sub-paragraph b of this article;

b "property" includes property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title to or interest in such property;

c "instrumentalities" means any property used or intended to be used, in any manner, wholly or in part, to commit a criminal offence or criminal offences;

d "confiscation" means a penalty or a measure, ordered by a court following proceedings in relation to a criminal offence or criminal offences resulting in the final deprivation of property;

e "predicate offence" means any criminal offence as a result of which proceeds were generated that may become the subject of an offence as defined in Article 9 of this Convention.

g "freezing" or "seizure" means temporarily prohibiting the transfer, destruction, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

9 MONEY LAUNDERING OFFENCES

9.1.1 FATF Recommendations

Definitions

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; (including in relation to customs and excise duties and taxes);
- tax crimes (related to direct taxes and indirect taxes);
- 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.

Recommendation 3

Countries should criminalise money laundering on the basis of the Vienna Convention and 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.

Interpretative Note to Recommendation 3

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).
2. 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.
3. 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 that 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 that are punished by a minimum penalty of more than six months imprisonment.
4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.
5. 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.
6. 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.

7. Countries should ensure that:

- (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.
- (b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.
- (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.
- (d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

9.1.2 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 3

1. Each Party shall adopt such measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally:

- (a) (i) The production, manufacture, extraction, preparation, offering, offering for sale, distribution, sale, delivery on any terms whatsoever, brokerage, dispatch, dispatch in transit, transport, importation or exportation of any narcotic drug or any psychotropic substance contrary to the provisions of the 1961 Convention, the 1961 Convention as amended or the 1971 Convention;
 - (ii) The cultivation of opium poppy, coca bush or cannabis plant for the purpose of the production of narcotic drugs contrary to the provisions of the 1961 Convention and the 1961 Convention as amended;
 - (iii) The possession or purchase of any narcotic drug or psychotropic substance for the purpose of any of the activities enumerated in (i) above;
 - (iv) The manufacture, transport or distribution of equipment, materials or of substances listed in Table I and Table II, knowing that they are to be used in or for the illicit cultivation, production or manufacture of narcotic drugs or psychotropic substances;
 - (v) The organization, management or financing of any of the offences enumerated in (i), (ii), (iii) or (iv) above;
 - (b) (i) The conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with subparagraph (a) of this paragraph, or from an act of participation in such offence or offences, 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 an offence or offences to evade the legal consequences of his actions;
 - (ii) 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 an offence or offences established in accordance with subparagraph (a) of this paragraph or from an act of participation in such an offence or offences;
 - (c) Subject to its constitutional principles and the basic concepts of its legal system:
 - (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from an offence or offences established in accordance with subparagraph (a) of this paragraph or from an act of participation in such offence or offences;
 - (ii) The possession of equipment or materials or substances listed in Table I and Table II, knowing that they are being or are to be used in or for the illicit cultivation, production or manufacture of narcotic drugs or psychotropic substances;
 - (iii) Publicly inciting or inducing others, by any means, to commit any of the offences established in accordance with this article or to use narcotic drugs or psychotropic substances illicitly;
 - (iv) Participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.
2. Subject to its constitutional principles and the basic concepts of its legal system, each Party shall adopt such measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally, the possession, purchase or cultivation of narcotic drugs or psychotropic substances for personal consumption contrary to the provisions of the 1961 Convention, the 1961 Convention as amended or the 1971 Convention.
3. Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.
4. (a) Each Party shall make the commission of the offences established in accordance with paragraph 1 of this article liable to sanctions which take into account the grave nature of these offences, such as imprisonment or other forms of deprivation of liberty, pecuniary sanctions and confiscation.
- (b) The Parties may provide, in addition to conviction or punishment, for an offence established in accordance with paragraph 1 of this article, that the offender shall undergo measures such as treatment, education, aftercare, rehabilitation or social reintegration.

(c) Notwithstanding the preceding subparagraphs, in appropriate cases of a minor nature, the Parties may provide, as alternatives to conviction or punishment, measures such as education, rehabilitation or social reintegration, as well as, when the offender is a drug abuser, treatment and aftercare.

(d) The Parties may provide, either as an alternative to conviction or punishment, or in addition to conviction or punishment of an offence established in accordance with paragraph 2 of this article, measures for the treatment, education, aftercare, rehabilitation or social reintegration of the offender.

5. The Parties shall ensure that their courts and other competent authorities having jurisdiction can take into account factual circumstances which make the commission of the offences established in accordance with paragraph 1 of this article particularly serious, such as:

(a) The involvement in the offence of an organized criminal group to which the offender belongs;

(b) The involvement of the offender in other international organized criminal activities;

(c) The involvement of the offender in other illegal activities facilitated by commission of the offence;

(d) The use of violence or arms by the offender;

(e) The fact that the offender holds a public office and that the offence is connected with the office in question;

(f) The victimization or use of minors;

(g) The fact that the offence is committed in a penal institution or in an educational institution or social service facility or in their immediate vicinity or in other places to which school children and students resort for educational, sports and social activities;

(h) Prior conviction, particularly for similar offences, whether foreign or domestic, to the extent permitted under the domestic law of a Party.

6. The Parties shall endeavour to ensure that any discretionary legal powers under their domestic law relating to the prosecution of persons for offences established in accordance with this article are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

7. The Parties shall ensure that their courts or other competent authorities bear in mind the serious nature of the offences enumerated in paragraph 1 of this article and the circumstances enumerated in paragraph 5 of this article when considering the eventuality of early release or parole of persons convicted of such offences.

8. Each Party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence established in accordance with paragraph 1 of this article, and a longer period where the alleged offender has evaded the administration of justice.

9. Each Party shall take appropriate measures, consistent with its legal system, to ensure that a person charged with or convicted of an offence established in accordance with paragraph 1 of this article, who is found within its territory, is present at the necessary criminal proceedings.

10. For the purpose of co-operation among the Parties under this Convention, including, in particular, co-operation under articles 5, 6, 7 and 9, offences established in accordance with this article shall not be considered as fiscal offences or as political offences or regarded as politically motivated, without prejudice to the constitutional limitations and the fundamental domestic law of the Parties.

11. Nothing contained in this article shall affect the principle that the description of the offences to which it refers and of legal defences thereto is reserved to the domestic law of a Party and that such offences shall be prosecuted and punished in conformity with that law.

9.1.3 2000 UN Convention against Transnational Organized Crime

Article 5 - Criminalization of participation in an organized criminal group

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) Either or both of the following as criminal offences distinct from those involving the attempt or completion of the criminal activity:

(i) Agreeing with one or more other persons to commit a serious crime for a purpose relating directly or indirectly to the obtaining of a financial or other material benefit and, where required by domestic law, involving an act undertaken by one of the participants in furtherance of the agreement or involving an organized criminal group;

(ii) Conduct by a person who, with knowledge of either the aim and general criminal activity of an organized criminal group or its intention to commit the crimes in question, takes an active part in:

a. Criminal activities of the organized criminal group;

b. Other activities of the organized criminal group in the knowledge that his or her participation will contribute to the achievement of the above described criminal aim;

(b) Organizing, directing, aiding, abetting, facilitating or counselling the commission of serious crime involving an organized criminal group.

2. The knowledge, intent, aim, purpose or agreement referred to in paragraph 1 of this article may be inferred from objective factual circumstances.

3. States Parties whose domestic law requires involvement of an organized criminal group for purposes of the offences established in accordance with paragraph 1 (a) (i) of this article shall ensure that their domestic law covers all serious

crimes involving organized criminal groups. Such States Parties, as well as States Parties whose domestic law requires an act in furtherance of the agreement for purposes of the offences established in accordance with paragraph 1 (a) (i) of this article, shall so inform the Secretary-General of the United Nations at the time of their signature or of deposit of their instrument of ratification, acceptance or approval of or accession to this Convention.

Article 6 - Criminalization of the laundering of proceeds of crime

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(b) Subject to the basic concepts of its legal system:

(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

2. For purposes of implementing or applying paragraph 1 of this article:

(a) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences;

(b) Each State Party shall include as predicate offences all serious crime as defined in article 2 of this Convention and the offences established in accordance with articles 5, 8 and 23 of this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in such list a comprehensive range of offences associated with organized criminal groups;

(c) For the purposes of subparagraph (b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;

(d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;

(e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

(f) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

Article 8 - Criminalization of corruption

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) The promise, offering or giving to a public official, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties;

(b) The solicitation or acceptance by a public official, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties.

2. Each State Party shall consider adopting such legislative and other measures as may be necessary to establish as criminal offences conduct referred to in paragraph 1 of this article involving a foreign public official or international civil servant. Likewise, each State Party shall consider establishing as criminal offences other forms of corruption.

3. Each State Party shall also adopt such measures as may be necessary to establish as a criminal offence participation as an accomplice in an offence established in accordance with this article.

4. For the purposes of paragraph 1 of this article and article 9 of this Convention, "public official" shall mean a public official or a person who provides a public service as defined in the domestic law and as applied in the criminal law of the State Party in which the person in question performs that function.

9.1.4 2003 UN Convention against Corruption

Article 23 - Laundering of proceeds of crime

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

- (ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;
 - (b) Subject to the basic concepts of its legal system:
 - (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;
 - (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.
2. For purposes of implementing or applying paragraph 1 of this article:
- (a) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences;
 - (b) Each State Party shall include as predicate offences at a minimum a comprehensive range of criminal offences established in accordance with this Convention;
 - (c) For the purposes of subparagraph (b) above, predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;
 - (d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;
 - (e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence.

Article 24 - Concealment

Without prejudice to the provisions of article 23 of this Convention, each State Party shall consider adopting such legislative and other measures as may be necessary to establish as a criminal offence, when committed intentionally after the commission of any of the offences established in accordance with this Convention without having participated in such offences, the concealment or continued retention of property when the person involved knows that such property is the result of any of the offences established in accordance with this Convention.

Article 27 - Participation and attempt

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, participation in any capacity such as an accomplice, assistant or instigator in an offence established in accordance with this Convention.
2. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, any attempt to commit an offence established in accordance with this Convention.
3. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, the preparation for an offence established in accordance with this Convention.

Article 28- Knowledge, intent and purpose as elements of an offence

Knowledge, intent or purpose required as an element of an offence established in accordance with this Convention may be inferred from objective factual circumstances.

9.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 9 – Laundering offences

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as offences under its domestic law, when committed intentionally:
 - a the conversion or transfer of property, knowing that such property is proceeds, 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 the predicate offence to evade the legal consequences of his actions;
 - 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 proceeds;
 and, subject to its constitutional principles and the basic concepts of its legal system;
 - c the acquisition, possession or use of property, knowing, at the time of receipt, that such property was proceeds;
 - d participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.
- 2 For the purposes of implementing or applying paragraph 1 of this article:
 - a it shall not matter whether the predicate offence was subject to the criminal jurisdiction of the Party;

b it may be provided that the offences set forth in that paragraph do not apply to the persons who committed the predicate offence;

c knowledge, intent or purpose required as an element of an offence set forth in that paragraph may be inferred from objective, factual circumstances.

3 Each Party may adopt such legislative and other measures as may be necessary to establish as an offence under its domestic law all or some of the acts referred to in paragraph 1 of this article, in either or both of the following cases where the offender

a suspected that the property was proceeds, bought to have assumed that the property was proceeds.

4 Provided that paragraph 1 of this article applies to the categories of predicate offences in the appendix to the Convention, each State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that paragraph 1 of this article applies:

a only in so far as the predicate offence is punishable by deprivation of liberty or a detention order for a maximum of more than one year, or for those Parties that have a minimum threshold for offences in their legal system, in so far as the offence is punishable by deprivation of liberty or a detention order for a minimum of more than six months; and/or

b only to a list of specified predicate offences; and/or

c to a category of serious offences in the national law of the Party.

5 Each Party shall ensure that a prior or simultaneous conviction for the predicate offence is not a prerequisite for a conviction for money laundering.

6 Each Party shall ensure that a conviction for money laundering under this Article is possible where it is proved that the property, the object of paragraph 1.a or b of this article, originated from a predicate offence, without it being necessary to establish precisely which offence.

7 Each Party shall ensure that predicate offences for money laundering extend to conduct that occurred in another State, which constitutes an offence in that State, and which would have constituted a predicate offence had it occurred domestically. Each Party may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Article 11 – Previous decisions

Each Party shall adopt such legislative and other measures as may be necessary to provide for the possibility of taking into account, when determining the penalty, final decisions against a natural or legal person taken in another Party in relation to offences established in accordance with this Convention.

9.1.6 Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime

Article 2 – Penalties

Each Member State shall take the necessary steps consistent with its system of penalties to ensure that the offences referred to in Article 6(1) (a) and (b) of the 1990 Convention, as they result from the Article 1(b) of this framework Decision, are punishable by deprivation of liberty for a maximum of not less than 4 years.

10 PROVISIONAL MEASURES AND CONFISCATION

10.1.1 FATF Recommendations

Definitions

Confiscation The term confiscation, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

Ex Parte means proceeding without prior notification and participation of the affected party.

Freeze In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.

Non-conviction based confiscation means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.

Proceeds refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.

Seize means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.

Recommendation 4

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of *bona fide* third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) 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, or (d) property of corresponding value. Such measures should include the authority to: (a) identify, trace and evaluate property that 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 country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), 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.

Interpretative Note to Recommendation 4

Countries should establish mechanisms that will enable their competent authorities to effectively manage and, when necessary, dispose of, property that is frozen or seized, or has been confiscated. These mechanisms should be applicable both in the context of domestic proceedings, and pursuant to requests by foreign countries.

10.1.2 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 5

1. Each Party shall adopt such measures as may be necessary to enable confiscation of:

(a) Proceeds derived from offences established in accordance with article 3, paragraph 1, or property the value of which corresponds to that of such proceeds;

2. Each Party shall also adopt such measures as may be necessary to enable its competent authorities to identify, trace, and freeze or seize proceeds, property, instrumentalities or any other things referred to in paragraph 1 of this article, for the purpose of eventual confiscation.

3. In order to carry out the measures referred to in this article, each Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. A Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

6. (a) If proceeds have been transformed or converted into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

(b) If proceeds have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to seizure or freezing, be liable to confiscation up to the assessed value of the intermingled proceeds.

(c) Income or other benefits derived from:

(i) Proceeds;

(ii) Property into which proceeds have been transformed or converted; or

(iii) Property with which proceeds have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds.

7. Each Party may consider ensuring that the onus of proof be reversed regarding the lawful origin of alleged proceeds or other property liable to confiscation, to the extent that such action is consistent with the principles of its domestic law and with the nature of the judicial and other proceedings.

8. The provisions of this article shall not be construed as prejudicing the rights of *bona fide* third parties.

9. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a Party.

10.1.3 2000 UN Convention against Transnational Organized Crime

Article 12 - Confiscation and seizure

1. States Parties shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

2. States Parties shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

4. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

5. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

6. For the purposes of this article and article 13 of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. States Parties shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

7. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

8. The provisions of this article shall not be construed to prejudice the rights of *bona fide* third parties.

9. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

10.1.4 2003 UN Convention against Corruption

Article 31- Freezing, seizure and confiscation

1. Each State Party shall take, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences established in accordance with this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Convention.

2. Each State Party shall take such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

4. If such proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

5. If such proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

6. Income or other benefits derived from such proceeds of crime, from property into which such proceeds of crime have been transformed or converted or from property with which such proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

7. For the purpose of this article and article 55 of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

8. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of such alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the fundamental principles of their domestic law and with the nature of judicial and other proceedings.

9. The provisions of this article shall not be so construed as to prejudice the rights of bona fide third parties.

10. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

10.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 3 – Confiscation measures

1 Each Party shall adopt such legislative and other measures as may be necessary to enable it to confiscate instrumentalities and proceeds or property the value of which corresponds to such proceeds and laundered property.

2 Provided that paragraph 1 of this article applies to money laundering and to the categories of offences in the appendix to the Convention, each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that paragraph 1 of this article applies

a only in so far as the offence is punishable by deprivation of liberty or a detention order for a maximum of more than one year. However, each Party may make a declaration on this provision in respect of the confiscation of the proceeds from tax offences for the sole purpose of being able to confiscate such proceeds, both nationally and through international cooperation, under national and international tax-debt recovery legislation; and/or

b only to a list of specified offences.

3 Parties may provide for mandatory confiscation in respect of offences which are subject to the confiscation regime. Parties may in particular include in this provision the offences of money laundering, drug trafficking, trafficking in human beings and any other serious offence.

4 Each Party shall adopt such legislative or other measures as may be necessary to require that, in respect of a serious offence or offences as defined by national law, an offender demonstrates the origin of alleged proceeds or other property liable to confiscation to the extent that such a requirement is consistent with the principles of its domestic law.

Article 4 – Investigative and provisional measures

Each Party shall adopt such legislative and other measures as may be necessary to enable it to identify, trace, freeze or seize rapidly property which is liable to confiscation pursuant to Article 3, in order in particular to facilitate the enforcement of a later confiscation.

Article 5 – Freezing, seizure and confiscation

Each Party shall adopt such legislative and other measures as may be necessary to ensure that the measures to freeze, seize and confiscate also encompass:

- a the property into which the proceeds have been transformed or converted;
- b property acquired from legitimate sources, if proceeds have been intermingled, in whole or in part, with such property, up to the assessed value of the intermingled proceeds;
- c income or other benefits derived from proceeds, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, up to the assessed value of the intermingled proceeds, in the same manner and to the same extent as proceeds.

Article 6 – Management of frozen or seized property

Each Party shall adopt such legislative or other measures as may be necessary to ensure proper management of frozen or seized property in accordance with Articles 4 and 5 of this Convention.

Article 7 – Investigative powers and techniques

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized in order to carry out the actions referred to in Articles 3, 4 and 5. A Party shall not decline to act under the provisions of this article on grounds of bank secrecy.

2 Without prejudice to paragraph 1, each Party shall adopt such legislative and other measures as may be necessary to enable it to:

- a determine whether a natural or legal person is a holder or beneficial owner of one or more accounts, of whatever nature, in any bank located in its territory and, if so obtain all of the details of the identified accounts;
 - b obtain the particulars of specified bank accounts and of banking operations which have been carried out during a specified period through one or more specified accounts, including the particulars of any sending or recipient account;
 - c monitor, during a specified period, the banking operations that are being carried out through one or more identified accounts; and,
 - d ensure that banks do not disclose to the bank customer concerned or to other third persons that information has been sought or obtained in accordance with sub-paragraphs a, b, or c, or that an investigation is being carried out.
- Parties shall consider extending this provision to accounts held in non-bank financial institutions.

Article 14 – Postponement of domestic suspicious transactions

Each Party shall adopt such legislative and other measures as may be necessary to permit urgent action to be taken by the FIU or, as appropriate, by any other competent authorities or body, when there is a suspicion that a transaction is related to money laundering, to suspend or withhold consent to a transaction going ahead in order to analyse the transaction and confirm the suspicion. Each party may restrict such a measure to cases where a suspicious transaction report has been submitted. The maximum duration of any suspension or withholding of consent to a transaction shall be subject to any relevant provisions in national law.

10.1.6 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)

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.

10.1.7 Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime

Article 3 - Value confiscation

Each Member State shall take the necessary steps to ensure that its legislation and procedures on the confiscation of the proceeds of crime also allow, at least in cases where these proceeds cannot be seized, for the confiscation of property

the value of which corresponds to such proceeds, both in purely domestic proceedings and in proceedings instituted at the request of another Member State, including requests for the enforcement of foreign confiscation orders. However, Member States may exclude the confiscation of property the value of which corresponds to the proceeds of crime in cases in which that value would be less than EUR 4000.

The words "property", "proceeds" and "confiscation" shall have the same meaning as in Article 1 of the 1990 Convention.

11 BEARER SHARES, TRUSTS AND CORPORATE CRIMINAL LIABILITY

11.1.1 FATF Recommendations

Definitions

Bearer shares refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.

Express trust refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).

Trustee The terms trust and trustee should be understood as described in and consistent with Article 2 of the Hague Convention on the law applicable to trusts and their recognition.²⁴ Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family).

Recommendation 24

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. 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 or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

Interpretative Note to Recommendation 24

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information²⁵) that are created²⁶ in the country. Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. It is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective.

2. As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

(a) identify and describe the different types, forms and basic features of legal persons in the country.

(b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;

(c) make the above information publicly available; and

(d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country.

3. In order to determine who the beneficial owners of a company are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.

4. All companies created in a country should be registered in a company registry.²⁷ Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic

²⁴ Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics - a) the assets constitute a separate fund and are not a part of the trustee's own estate; b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee; c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law. The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

²⁵ Beneficial ownership information for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (e.g. 25%).

²⁶ References to creating a legal person, include incorporation of companies or any other mechanism that is used.

²⁷ "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

information on a company that needs to be obtained and recorded by the company²⁸ as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

(a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors; and

(b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder²⁹ and categories of shares (including the nature of the associated voting rights).

5. The company registry should record all the basic information set out in paragraph 4(a) above.

6. The company should maintain the basic information set out in paragraph 4(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

7. Countries should ensure that either: (a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority.

8. In order to meet the requirements in paragraph 7, countries should use one or more of the following mechanisms:

(a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

(b) Requiring companies to take reasonable measures³⁰ to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22³¹; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators); (iii) information held by the company as required above in Section A; and (iv) available information on companies listed on a stock exchange, where disclosure requirements (either by stock exchange rules or through law or enforceable means) impose requirements to ensure adequate transparency of beneficial ownership.

9. Regardless of which of the above mechanisms are used, countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner. This should include:

(a) Requiring that one or more natural persons resident in the country is authorised by the company³², and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

(b) Requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

(c) Other comparable measures, specifically identified by the country, which can effectively ensure cooperation.

10. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

11. Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis. Countries should require that any available information referred to in paragraph 7 is accurate and is kept as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

12. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

13. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above.

14. Countries should take measures to prevent the misuse of bearer shares and bearer share warrants, for example by applying one or more of the following mechanisms: (a) prohibiting them; (b) converting them into registered shares or share warrants (for example through dematerialisation); (c) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary; or (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity.

²⁸ The information can be recorded by the company itself or by a third person under the company's responsibility.

²⁹ This is applicable to the nominal owner of all registered shares.

³⁰ Measures taken should be proportionate to the level of risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders.

³¹ Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

³² Members of the company's board or senior management may not require specific authorisation by the company.

15. Countries should take measures to prevent the misuse of nominee shares and nominee directors, for example by applying one or more of the following mechanisms: (a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or (b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request.

16. In relation to foundations, Anstalt, and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures.

17. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and current by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and current beneficial ownership information for such legal persons.

18. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

19. Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

Recommendation 25

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. 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 should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

Interpretative Note to Recommendation 25

1. Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.

2. All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when, as a trustee, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust³³; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

3. Countries are encouraged to ensure that other relevant authorities, persons and entities hold information on all trusts with which they have a relationship. Potential sources of information on trusts, trustees, and trust assets are:

(a) Registries (e.g. a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets.

(b) Other competent authorities that hold information on trusts and trustees (e.g. tax authorities which collect information on assets and income relating to trusts).

(c) Other agents and service providers to the trust, including investment advisors or managers, lawyers, or trust and company service providers.

4. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the information held by trustees and other parties, in particular information held by financial institutions and DNFBPs on: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

³³ Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

5. Professional trustees should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust ceases. Countries are encouraged to require non-professional trustees and the other authorities, persons and entities mentioned in paragraph 3 above to maintain the information for at least five years.
6. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and be as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.
7. Countries should consider measures to facilitate access to any information on trusts that is held by the other authorities, persons and entities referred to in paragraph 3, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.
8. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 2 and 6 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).
9. As regards other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified above in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities.
10. Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.
11. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 2, 6 and (where applicable) 5; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.³⁴ Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in paragraphs 1 and 5.

11.1.2 2000 UN Convention against Transnational Organized Crime

Article 10 - Liability of legal persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in serious crimes involving an organized criminal group and for the offences established in accordance with articles 5, 6, 8 and 23 of this Convention.
2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.
3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.
4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

11.1.3 2003 UN Convention against Corruption

Article 26 - Liability of legal persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention.
2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.
3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.
4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

³⁴ This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

11.1.4 Basel Committee on Banking Supervision - Customer due diligence

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.

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.

11.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 10 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for the criminal offences of money laundering established in accordance with this Convention, committed for their benefit by any natural 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; or
- b an authority to take decisions on behalf of the legal person; or
- c an authority to exercise control within the legal person,

as well as for involvement of such a natural person as accessory or instigator in the above-mentioned offences.

2 Apart from the cases already provided for in paragraph 1, each Party shall take the necessary measures to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of the criminal offences mentioned in paragraph 1 for the benefit of that legal person by a natural person under its authority.

3 Liability of a legal person under this Article shall not exclude criminal proceedings against natural persons who are perpetrators, instigators of, or accessories to, the criminal offences mentioned in paragraph 1.

4 Each Party shall ensure that legal persons held liable in accordance with this Article, shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

11.1.6 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)

Article 39

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 paragraph 3, Member States shall ensure that legal persons can be held 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.

11.2 Shell banks

11.2.1 FATF Recommendations

Recommendation 26

...

Countries should not approve the establishment, or continued operation, of shell banks.

11.2.2 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist

Article 3

(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 13

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.

12 NATIONAL CO-OPERATION

12.1.1 FATF Recommendations

Recommendation 2

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies. Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

Recommendation 33

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs 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 cooperation.

Recommendation 34

The competent authorities, supervisors and SRBs 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.

12.1.2 2000 UN Convention against Transnational Organized Crime

Article 7 - Measures to combat money-laundering

1. Each State Party:

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

12.1.3 2003 UN Convention against Corruption

Article 14 - Measures to prevent money-laundering

1. Each State Party shall:

(b) Without prejudice to article 46 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering.

Article 37 - Cooperation with law enforcement authorities

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in the commission of an offence established in accordance with this Convention to supply information useful to competent authorities for investigative and evidentiary purposes and to provide factual, specific help to competent authorities that may contribute to depriving offenders of the proceeds of crime and to recovering such proceeds.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence established in accordance with this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence established in accordance with this Convention.

4. Protection of such persons shall be, mutatis mutandis, as provided for in article 32 of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

Article 38 - Cooperation between national authorities

Each State Party shall take such measures as may be necessary to encourage, in accordance with its domestic law, cooperation between, on the one hand, its public authorities, as well as its public officials, and, on the other hand, its authorities responsible for investigating and prosecuting criminal offences. Such cooperation may include:

- (a) Informing the latter authorities, on their own initiative, where there are reasonable grounds to believe that any of the offences established in accordance with articles 15, 21 and 23 of this Convention has been committed; or
- (b) Providing, upon request, to the latter authorities all necessary information.

Article 39 - Cooperation between national authorities and the private sector

1. Each State Party shall take such measures as may be necessary to encourage, in accordance with its domestic law, cooperation between national investigating and prosecuting authorities and entities of the private sector, in particular financial institutions, relating to matters involving the commission of offences established in accordance with this Convention.

2. Each State Party shall consider encouraging its nationals and other persons with a habitual residence in its territory to report to the national investigating and prosecuting authorities the commission of an offence established in accordance with this Convention.

Article 40 - Bank secrecy

Each State Party shall ensure that, in the case of domestic criminal investigations of offences established in accordance with this Convention, there are appropriate mechanisms available within its domestic legal system to overcome obstacles that may arise out of the application of bank secrecy laws.

Article 41- Criminal record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence established in accordance with this Convention.

12.1.4 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)

Article 33

1. Member States shall ensure that they are able to review the 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.

13 INTERNATIONAL CO-OPERATION

13.1 Mutual legal assistance – Law enforcement co-operation

13.1.1 FATF Recommendations

Definitions

Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).

Recommendation 37

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. 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 timely prioritization and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.
- (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.
- (e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality. Where dual criminality is required for mutual legal assistance, 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. Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

- (a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and
- (b) a broad range of other powers and investigative techniques; 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.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means.

Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Recommendation 40

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts. Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

Interpretative note to Recommendation 40

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.
2. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:
 - (a) the request is also considered to involve fiscal matters; and/or
 - (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or
 - (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or
 - (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.
3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.
4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry³⁵, consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.
5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.
6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.
7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.
8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.
9. FIUs should have the power to exchange:
 - (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and
 - (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.
10. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent

³⁵ Information may be disclosed if such disclosure is required to carry out the request for cooperation.

with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

11. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:

(a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors.

(b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.

(c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

12. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

13. Any dissemination of information exchanged or use of that information for supervisory and non-supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

14. Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

15. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

16. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

17. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

18. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

13.1.2 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 7

1. The Parties shall afford one another, pursuant to this article, the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to criminal offences established in accordance with article 3, paragraph 1.

2. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

(a) Taking evidence or statements from persons;

(b) Effecting service of judicial documents;

(c) Executing searches and seizures;

(d) Examining objects and sites;

(e) Providing information and evidentiary items;

(f) Providing originals or certified copies of relevant documents and records, including bank, financial, corporate or business records;

- (g) Identifying or tracing proceeds, property, instrumentalities or other things for evidentiary purposes.
3. The Parties may afford one another any other forms of mutual legal assistance allowed by the domestic law of the requested Party.
4. Upon request, the Parties shall facilitate or encourage, to the extent consistent with their domestic law and practice, the presence or availability of persons, including persons in custody, who consent to assist in investigations or participate in proceedings.
5. A Party shall not decline to render mutual legal assistance under this article on the ground of bank secrecy.
6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, which governs or will govern, in whole or in part, mutual legal assistance in criminal matters.
7. Paragraphs 8 to 19 of this article shall apply to requests made pursuant to this article if the Parties in question are not bound by a treaty of mutual legal assistance. If these Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the Parties agree to apply paragraphs 8 to 19 of this article in lieu thereof.
8. Parties shall designate an authority, or when necessary authorities, which shall have the responsibility and power to execute requests for mutual legal assistance or to transmit them to the competent authorities for execution. The authority or the authorities designated for this purpose shall be notified to the Secretary-General. Transmission of requests for mutual legal assistance and any communication related thereto shall be effected between the authorities designated by the Parties; this requirement shall be without prejudice to the right of a Party to require that such requests and communications be addressed to it through the diplomatic channel and, in urgent circumstances, where the Parties agree, through channels of the International Criminal Police Organization, if possible.
9. Requests shall be made in writing in a language acceptable to the requested Party. The language or languages acceptable to each Party shall be notified to the Secretary-General. In urgent circumstances, and where agreed by the Parties, requests may be made orally, but shall be confirmed in writing forthwith.
10. A request for mutual legal assistance shall contain:
- (a) The identity of the authority making the request;
 - (b) The subject matter and nature of the investigation, prosecution or proceeding to which the request relates, and the name and the functions of the authority conducting such investigation, prosecution or proceeding;
 - (c) A summary of the relevant facts, except in respect of requests for the purpose of service of judicial documents;
 - (d) A description of the assistance sought and details of any particular procedure the requesting Party wishes to be followed;
 - (e) Where possible, the identity, location and nationality of any person concerned;
 - (f) The purpose for which the evidence, information or action is sought.
11. The requested Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.
12. A request shall be executed in accordance with the domestic law of the requested Party and, to the extent not contrary to the domestic law of the requested Party and where possible, in accordance with the procedures specified in the request.
13. The requesting Party shall not transmit nor use information or evidence furnished by the requested Party for investigations, prosecutions or proceedings other than those stated in the request without the prior consent of the requested Party.
14. The requesting Party may require that the requested Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting Party.
15. Mutual legal assistance may be refused:
- (a) If the request is not made in conformity with the provisions of this article;
 - (b) If the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordure public* or other essential interests;
 - (c) If the authorities of the requested Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or proceedings under their own jurisdiction;
 - (d) If it would be contrary to the legal system of the requested Party relating to mutual legal assistance for the request to be granted.
16. Reasons shall be given for any refusal of mutual legal assistance.
17. Mutual legal assistance may be postponed by the requested Party on the ground that it interferes with an ongoing investigation, prosecution or proceeding. In such a case, the requested Party shall consult with the requesting Party to determine if the assistance can still be given subject to such terms and conditions as the requested Party deems necessary.
18. A witness, expert or other person who consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting Party, shall not be prosecuted, detained, punished or subjected to any other restriction of his personal liberty in that territory in respect of acts, omissions or convictions prior to his departure from the territory of the requested Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of fifteen consecutive days, or for any period agreed upon by the Parties, from the date on which he has been officially informed that his presence is no longer required by the judicial authorities, an

opportunity of leaving, has nevertheless remained voluntarily in the territory or, having left it, has returned of his own free will.

19. The ordinary costs of executing a request shall be borne by the requested Party, unless otherwise agreed by the Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the Parties shall consult to determine the terms and conditions under which the request will be executed as well as the manner in which the costs shall be borne.

20. The Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to, or enhance the provisions of this article.

13.1.3 2000 UN Convention against Transnational Organized Crime

Article 7 - Measures to combat money-laundering

1. Each State Party:

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

4. States Parties shall endeavour to develop and promote global, regional, subregional and bilateral cooperation among judicial, law enforcement and financial regulatory authorities in order to combat money-laundering.

Article 18 - Mutual legal assistance

1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention as provided for in article 3 and shall reciprocally extend to one another similar assistance where the requesting State Party has reasonable grounds to suspect that the offence referred to in article 3, paragraph 1 (a) or (b), is transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State Party and that the offence involves an organized criminal group.

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 10 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

- (a) Taking evidence or statements from persons;
- (b) Effecting service of judicial documents;
- (c) Executing searches and seizures, and freezing;
- (d) Examining objects and sites;
- (e) Providing information, evidentiary items and expert evaluations;
- (f) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;
- (g) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;
- (h) Facilitating the voluntary appearance of persons in the requesting State Party;
- (i) Any other type of assistance that is not contrary to the domestic law of the requested State Party.

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 9 to 29 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this article in lieu thereof. States Parties are strongly encouraged to apply these paragraphs if they facilitate cooperation.

8. States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.

9. States Parties may decline to render mutual legal assistance pursuant to this article on the ground of absence of dual criminality. However, the requested State Party may, when it deems appropriate, provide assistance, to the extent it decides at its discretion, irrespective of whether the conduct would constitute an offence under the domestic law of the requested State Party.

10. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for investigations, prosecutions or judicial proceedings in relation to offences covered by this Convention may be transferred if the following conditions are met:

(a) The person freely gives his or her informed consent;

(b) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.

11. For the purposes of paragraph 10 of this article:

(a) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State Party from which the person was transferred;

(b) The State Party to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;

(c) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition proceedings for the return of the person;

(d) The person transferred shall receive credit for service of the sentence being served in the State from which he or she was transferred for time spent in the custody of the State Party to which he or she was transferred.

12. Unless the State Party from which a person is to be transferred in accordance with paragraphs 10 and 11 of this article so agrees, that person, whatever his or her nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to his or her departure from the territory of the State from which he or she was transferred.

13. Each State Party shall designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory. Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority. The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.

14. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally, but shall be confirmed in writing forthwith.

15. A request for mutual legal assistance shall contain:

(a) The identity of the authority making the request;

(b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;

(c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;

(d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;

(e) Where possible, the identity, location and nationality of any person concerned; and

(f) The purpose for which the evidence, information or action is sought

16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.

17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.

18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by video conference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party.

19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.

21. Mutual legal assistance may be refused:

(a) If the request is not made in conformity with the provisions of this article;

(b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests;

(c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;

(d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

22. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

23. Reasons shall be given for any refusal of mutual legal assistance.

24. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requested State Party shall respond to reasonable requests by the requesting State Party on progress of its handling of the request. The requesting State Party shall promptly inform the requested State Party when the assistance sought is no longer required.

25. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.

26. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 25 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those conditions, it shall comply with the conditions.

27. Without prejudice to the application of paragraph 12 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in that territory in respect of acts, omissions or convictions prior to his or her departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of fifteen consecutive days or for any period agreed upon by the States Parties from the date on which he or she has been officially informed that his or her presence is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of his or her own free will.

28. The ordinary costs of executing a request shall be borne by the requested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the States Parties shall consult to determine the terms and conditions under which the request will be executed, as well as the manner in which the costs shall be borne.

29. The requested State Party:

(a) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;

(b) May, at its discretion, provide to the requesting State Party in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.

30. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.

Article 21 - Transfer of criminal proceedings

States Parties shall consider the possibility of transferring to one another proceedings for the prosecution of an offence covered by this Convention in cases where such transfer is considered to be in the interests of the proper administration of justice, in particular in cases where several jurisdictions are involved, with a view to concentrating the prosecution.

Article 26 - Measures to enhance cooperation with law enforcement authorities

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in organized criminal groups:

(a) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:

(i) The identity, nature, composition, structure, location or activities of organized criminal groups;

(ii) Links, including international links, with other organized criminal groups;

(iii) Offences that organized criminal groups have committed or may commit;

(b) To provide factual, concrete help to competent authorities that may contribute to depriving organized criminal groups of their resources or of the proceeds of crime.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

4. Protection of such persons shall be as provided for in article 24 of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

Article 27 - Law enforcement cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences covered by this Convention. Each State Party shall, in particular, adopt effective measures:

(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

(b) To cooperate with other States Parties in conducting inquiries with respect to offences covered by this Convention concerning:

(i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

(ii) The movement of proceeds of crime or property derived from the commission of such offences;

(iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(c) To provide, when appropriate, necessary items or quantities of substances for analytical or investigative purposes;

(d) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;

(e) To exchange information with other States Parties on specific means and methods used by organized criminal groups, including, where applicable, routes and conveyances and the use of false identities, altered or false documents or other means of concealing their activities;

(f) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences covered by this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the Parties may consider this Convention as the basis for mutual law enforcement cooperation in respect of the offences covered by this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

3. States Parties shall endeavour to cooperate within their means to respond to transnational organized crime committed through the use of modern technology.

13.1.4 2003 UN Convention against Corruption

Article 14 - Measures to prevent money-laundering

1. Each State Party shall:

(b) Without prejudice to article 46 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering.

5. States Parties shall endeavour to develop and promote global, regional, subregional and bilateral cooperation among judicial, law enforcement and financial regulatory authorities in order to combat money-laundering.

Article 46 - Mutual legal assistance

1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention.

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 26 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

- (a) Taking evidence or statements from persons;
- (b) Effecting service of judicial documents;
- (c) Executing searches and seizures, and freezing;
- (d) Examining objects and sites;
- (e) Providing information, evidentiary items and expert evaluations;
- (f) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;
- (g) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;
- (h) Facilitating the voluntary appearance of persons in the requesting State Party;
- (i) Any other type of assistance that is not contrary to the domestic law of the requested State Party;
- (j) Identifying, freezing and tracing proceeds of crime in accordance with the provisions of chapter V of this Convention;
- (k) The recovery of assets, in accordance with the provisions of chapter V of this Convention.

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 9 to 29 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this article in lieu thereof. States Parties are strongly encouraged to apply those paragraphs if they facilitate cooperation.

8. States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.

9. (a) A requested State Party, in responding to a request for assistance pursuant to this article in the absence of dual criminality, shall take into account the purposes of this Convention, as set forth in article 1;

(b) States Parties may decline to render assistance pursuant to this article on the ground of absence of dual criminality. However, a requested State Party shall, where consistent with the basic concepts of its legal system, render assistance that does not involve coercive action. Such assistance may be refused when requests involve matters of a *de minimis* nature or matters for which the cooperation or assistance sought is available under other provisions of this Convention;

- (c) Each State Party may consider adopting such measures as may be necessary to enable it to provide a wider scope of assistance pursuant to this article in the absence of dual criminality.
10. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for investigations, prosecutions or judicial proceedings in relation to offences covered by this Convention may be transferred if the following conditions are met:
- (a) The person freely gives his or her informed consent;
 - (b) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.
11. For the purposes of paragraph 10 of this article:
- (a) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State Party from which the person was transferred;
 - (b) The State Party to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;
 - (c) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition proceedings for the return of the person;
 - (d) The person transferred shall receive credit for service of the sentence being served in the State from which he or she was transferred for time spent in the custody of the State Party to which he or she was transferred.
12. Unless the State Party from which a person is to be transferred in accordance with paragraphs 10 and 11 of this article so agrees, that person, whatever his or her nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to his or her departure from the territory of the State from which he or she was transferred.
13. Each State Party shall designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory. Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority. The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.
14. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally but shall be confirmed in writing forthwith.
15. A request for mutual legal assistance shall contain:
- (a) The identity of the authority making the request;
 - (b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;
 - (c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;
 - (d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;
 - (e) Where possible, the identity, location and nationality of any person concerned; and
 - (f) The purpose for which the evidence, information or action is sought.
16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.
17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.
18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by video conference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties

may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party.

19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.

21. Mutual legal assistance may be refused:

(a) If the request is not made in conformity with the provisions of this article;

(b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests;

(c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;

(d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

22. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

23. Reasons shall be given for any refusal of mutual legal assistance.

24. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requesting State Party may make reasonable requests for information on the status and progress of measures taken by the requested State Party to satisfy its request. The requested State Party shall respond to reasonable requests by the requesting State Party on the status, and progress in its handling, of the request. The requesting State Party shall promptly inform the requested State Party when the assistance sought is no longer required.

25. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.

26. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 25 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those conditions, it shall comply with the conditions.

27. Without prejudice to the application of paragraph 12 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of his or her personal liberty in that territory in respect of acts, omissions or convictions prior to his or her departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of fifteen consecutive days or for any period agreed upon by the States Parties from the date on which he or she has been officially informed that his or her presence is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of his or her own free will.

28. The ordinary costs of executing a request shall be borne by the requested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the States Parties shall consult to determine the terms and conditions under which the request will be executed, as well as the manner in which the costs shall be borne.

29. The requested State Party:

(a) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;

(b) May, at its discretion, provide to the requesting State Party in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.

30. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.

Article 47 - Transfer of criminal proceedings

States Parties shall consider the possibility of transferring to one another proceedings for the prosecution of an offence established in accordance with this Convention in cases where such transfer is considered to be in the interests of the proper administration of justice, in particular in cases where several jurisdictions are involved, with a view to concentrating the prosecution.

Article 48 - Law enforcement cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences covered by this Convention. States Parties shall, in particular, take effective measures:

(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

(b) To cooperate with other States Parties in conducting inquiries with respect to offences covered by this Convention concerning:

(i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

(ii) The movement of proceeds of crime or property derived from the commission of such offences;

(iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(c) To provide, where appropriate, necessary items or quantities of substances for analytical or investigative purposes;

(d) To exchange, where appropriate, information with other States Parties concerning specific means and methods used to commit offences covered by this Convention, including the use of false identities, forged, altered or false documents and other means of concealing activities;

(e) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;

(f) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences covered by this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the States Parties may consider this Convention to be the basis for mutual law enforcement cooperation in respect of the offences covered by this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

3. States Parties shall endeavour to cooperate within their means to respond to offences covered by this Convention committed through the use of modern technology.

13.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 15 – General principles and measures for international co-operation

1 The Parties shall mutually co-operate with each other to the widest extent possible for the purposes of investigations and proceedings aiming at the confiscation of instrumentalities and proceeds.

2 Each Party shall adopt such legislative or other measures as may be necessary to enable it to comply, under the conditions provided for in this chapter, with requests:

a for confiscation of specific items of property representing proceeds or instrumentalities, as well as for confiscation of proceeds consisting in a requirement to pay a sum of money corresponding to the value of proceeds;

b for investigative assistance and provisional measures with a view to either form of confiscation referred to under a above.

3 Investigative assistance and provisional measures sought in paragraph 2.b shall be carried out as permitted by and in accordance with the internal law of the requested Party. Where the request concerning one of these measures specifies formalities or procedures which are necessary under the law of the requesting Party, even if unfamiliar to the requested Party, the latter shall comply with such requests to the extent that the action sought is not contrary to the fundamental principles of its law.

4 Each Party shall adopt such legislative or other measures as may be necessary to ensure that the requests coming from other Parties in order to identify, trace, freeze or seize the proceeds and instrumentalities, receive the same priority as those made in the framework of internal procedures.

Article 16 – Obligation to assist

The Parties shall afford each other, upon request, the widest possible measure of assistance in the identification and tracing of instrumentalities, proceeds and other property liable to confiscation. Such assistance shall include any measure providing and securing evidence as to the existence, location or movement, nature, legal status or value of the aforementioned property.

Article 17 – Requests for information on bank accounts

1 Each Party shall, under the conditions set out in this article, take the measures necessary to determine, in answer to a request sent by another Party, whether a natural or legal person that is the subject of a criminal investigation holds or controls one or more accounts, of whatever nature, in any bank located in its territory and, if so, provide the particulars of the identified accounts.

2 The obligation set out in this article shall apply only to the extent that the information is in the possession of the bank keeping the account.

3 In addition to the requirements of Article 37, the requesting party shall, in the request:

a state why it considers that the requested information is likely to be of substantial value for the purpose of the criminal investigation into the offence;

b state on what grounds it presumes that banks in the requested Party hold the account and specify, to the widest extent possible, which banks and/or accounts may be involved; and

c include any additional information available which may facilitate the execution of the request.

4 The requested Party may make the execution of such a request dependant on the same conditions as it applies in respect of requests for search and seizure.

5 Each State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that this article applies only to the categories of offences specified in the list contained in the appendix to this Convention.

6 Parties may extend this provision to accounts held in non-bank financial institutions. Such extension may be made subject to the principle of reciprocity.

Article 18 – Requests for information on banking transactions

1 On request by another Party, the requested Party shall provide the particulars of specified bank accounts and of banking operations which have been carried out during a specified period through one or more accounts specified in the request, including the particulars of any sending or recipient account.

2 The obligation set out in this article shall apply only to the extent that the information is in the possession of the bank holding the account.

3 In addition to the requirements of Article 37, the requesting Party shall in its request indicate why it considers the requested information relevant for the purpose of the criminal investigation into the offence.

4 The requested Party may make the execution of such a request dependant on the same conditions as it applies in respect of requests for search and seizure.

5 Parties may extend this provision to accounts held in non-bank financial institutions. Such extension may be made subject to the principle of reciprocity.

Article 19 – Requests for the monitoring of banking transactions

1 Each Party shall ensure that, at the request of another Party, it is able to monitor, during a specified period, the banking operations that are being carried out through one or more accounts specified in the request and communicate the results thereof to the requesting Party.

2 In addition to the requirements of Article 37, the requesting Party shall in its request indicate why it considers the requested information relevant for the purpose of the criminal investigation into the offence.

3 The decision to monitor shall be taken in each individual case by the competent authorities of the requested Party, with due regard for the national law of that Party.

4 The practical details regarding the monitoring shall be agreed between the competent authorities of the requesting and requested Parties.

5 Parties may extend this provision to accounts held in non-bank financial institutions.

Article 20 – Spontaneous information

Without prejudice to its own investigations or proceedings, a Party may without prior request forward to another Party information on instrumentalities and proceeds, when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings or might lead to a request by that Party under this chapter.

Article 33 – Central authority

1 The Parties shall designate a central authority or, if necessary, authorities, which shall be responsible for sending and answering requests made under this chapter, the execution of such requests or the transmission of them to the authorities competent for their execution.

2 Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of paragraph 1 of this article.

Article 34 – Direct communication

- 1 The central authorities shall communicate directly with one another.
- 2 In the event of urgency, requests or communications under this chapter may be sent directly by the judicial authorities, including public prosecutors, of the requesting Party to such authorities of the requested Party. In such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
- 3 Any request or communication under paragraphs 1 and 2 of this article may be made through the International Criminal Police Organisation (Interpol).
- 4 Where a request is made pursuant to paragraph 2 of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
- 5 Requests or communications under Section 2 of this chapter, which do not involve coercive action, may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- 6 Draft requests or communications under this chapter may be sent directly by the judicial authorities of the requesting Party to such authorities of the requested Party prior to a formal request to ensure that it can be dealt with efficiently upon receipt and contains sufficient information and supporting documentation for it to meet the requirements of the legislation of the requested Party.

Article 35 – Form of request and languages

- 1 All requests under this chapter shall be made in writing. They may be transmitted electronically, or by any other means of telecommunication, provided that the requesting Party is prepared, upon request, to produce at any time a written record of such communication and the original. However each Party may, at any time, by a declaration addressed to the Secretary General of the Council of Europe, indicate the conditions in which it is ready to accept and execute requests received electronically or by any other means of communication.
- 2 Subject to the provisions of paragraph 3 of this article, translations of the requests or supporting documents shall not be required.
- 3 At the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, any State or the European Community may communicate to the Secretary General of the Council of Europe a declaration that it reserves the right to require that requests made to it and documents supporting such requests be accompanied by a translation into its own language or into one of the official languages of the Council of Europe or into such one of these languages as it shall indicate. It may on that occasion declare its readiness to accept translations in any other language as it may specify. The other Parties may apply the reciprocity rule.

Article 36 – Legalisation

Documents transmitted in application of this chapter shall be exempt from all legalisation formalities.

Article 37 – Content of request

- 1 Any request for co-operation under this chapter shall specify:
 - a the authority making the request and the authority carrying out the investigations or proceedings;
 - b the object of and the reason for the request;
 - c the matters, including the relevant facts (such as date, place and circumstances of the offence) to which the investigations or proceedings relate, except in the case of a request for notification;
 - d insofar as the co-operation involves coercive action:
 - i the text of the statutory provisions or, where this is not possible, a statement of the relevant law applicable; and
 - ii an indication that the measure sought or any other measures having similar effects could be taken in the territory of the requesting Party under its own law;
 - e where necessary and in so far as possible:
 - i details of the person or persons concerned, including name, date and place of birth, nationality and location, and, in the case of a legal person, its seat; and
 - ii the property in relation to which co-operation is sought, its location, its connection with the person or persons concerned, any connection with the offence, as well as any available information about other persons, interests in the property; and
 - f any particular procedure the requesting Party wishes to be followed.
- 2 A request for provisional measures under Section 3 in relation to seizure of property on which a confiscation order consisting in the requirement to pay a sum of money may be realised shall also indicate a maximum amount for which recovery is sought in that property.
- 3 In addition to the indications mentioned in paragraph 1, any request under Section 4 shall contain:
 - a in the case of Article 23, paragraph 1.a:
 - i a certified true copy of the confiscation order made by the court in the requesting Party and a statement of the grounds on the basis of which the order was made, if they are not indicated in the order itself;
 - ii an attestation by the competent authority of the requesting Party that the confiscation order is enforceable and not subject to ordinary means of appeal;

- iii information as to the extent to which the enforcement of the order is requested; and
- iv information as to the necessity of taking any provisional measures;
- b in the case of Article 23, paragraph 1.b, a statement of the facts relied upon by the requesting Party sufficient to enable the requested Party to seek the order under its domestic law;
- c when third parties have had the opportunity to claim rights, documents demonstrating that this has been the case.

Article 38 – Defective requests

- 1 If a request does not comply with the provisions of this chapter or the information supplied is not sufficient to enable the requested Party to deal with the request, that Party may ask the requesting Party to amend the request or to complete it with additional information.
- 2 The requested Party may set a time-limit for the receipt of such amendments or information.
- 3 Pending receipt of the requested amendments or information in relation to a request under Section 4 of this chapter, the requested Party may take any of the measures referred to in Sections 2 or 3 of this chapter.

Article 39 – Plurality of requests

- 1 Where the requested Party receives more than one request under Sections 3 or 4 of this chapter in respect of the same person or property, the plurality of requests shall not prevent that Party from dealing with the requests involving the taking of provisional measures.
- 2 In the case of plurality of requests under Section 4 of this chapter, the requested Party shall consider consulting the requesting Parties.

Article 40 – Obligation to give reasons

The requested Party shall give reasons for any decision to refuse, postpone or make conditional any co-operation under this chapter.

Article 41 – Information

- 1 The requested Party shall promptly inform the requesting Party of:
 - a the action initiated on a request under this chapter;
 - b the final result of the action carried out on the basis of the request;
 - c a decision to refuse, postpone or make conditional, in whole or in part, any co-operation under this chapter;
 - d any circumstances which render impossible the carrying out of the action sought or are likely to delay it significantly; and
 - e in the event of provisional measures taken pursuant to a request under Sections 2 or 3 of this chapter, such provisions of its domestic law as would automatically lead to the lifting of the provisional measure.
- 2 The requesting Party shall promptly inform the requested Party of:
 - a any review, decision or any other fact by reason of which the confiscation order ceases to be wholly or partially enforceable; and
 - b any development, factual or legal, by reason of which any action under this chapter is no longer justified.
- 3 Where a Party, on the basis of the same confiscation order, requests confiscation in more than one Party, it shall inform all Parties which are affected by an enforcement of the order about the request.

Article 42 – Restriction of use

- 1 The requested Party may make the execution of a request dependent on the condition that the information or evidence obtained will not, without its prior consent, be used or transmitted by the authorities of the requesting Party for investigations or proceedings other than those specified in the request.
- 2 Each State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by declaration addressed to the Secretary General of the Council of Europe, declare that, without its prior consent, information or evidence provided by it under this chapter may not be used or transmitted by the authorities of the requesting Party in investigations or proceedings other than those specified in the request.

Article 43 – Confidentiality

- 1 The requesting Party may require that the requested Party keep confidential the facts and substance of the request, except to the extent necessary to execute the request. If the requested Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting Party.
- 2 The requesting Party shall, if not contrary to basic principles of its national law and if so requested, keep confidential any evidence and information provided by the requested Party, except to the extent that its disclosure is necessary for the investigations or proceedings described in the request.
- 3 Subject to the provisions of its domestic law, a Party which has received spontaneous information under Article 20 shall comply with any requirement of confidentiality as required by the Party which supplies the information. If the other Party cannot comply with such requirement, it shall promptly inform the transmitting Party.

Article 44 – Costs

The ordinary costs of complying with a request shall be borne by the requested Party. Where costs of a substantial or extraordinary nature are necessary to comply with a request, the Parties shall consult in order to agree the conditions on which the request is to be executed and how the costs shall be borne.

Article 45 – Damages

1 When legal action on liability for damages resulting from an act or omission in relation to co-operation under this chapter has been initiated by a person, the Parties concerned shall consider consulting each other, where appropriate, to determine how to apportion any sum of damages due.

2 A Party which has become subject of a litigation for damages shall endeavour to inform the other Party of such litigation if that Party might have an interest in the case.

13.1.6 The 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU

Article 3 - Proceedings in connection with which mutual assistance is also to be afforded

1. Mutual assistance shall also be afforded in proceedings brought by the administrative authorities in respect of acts which are punishable under the national law of the requesting or the requested Member State, or both, by virtue of being infringements of the rules of law, and where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters.

2. Mutual assistance shall also be afforded in connection with criminal proceedings and proceedings as referred to in paragraph 1 which relate to offences or infringements for which a legal person may be held liable in the requesting Member State.

Article 4 - Formalities and procedures in the execution of requests for mutual assistance

1. Where mutual assistance is afforded, the requested Member State shall comply with the formalities and procedures expressly indicated by the requesting Member State, unless otherwise provided in this Convention and provided that such formalities and procedures are not contrary to the fundamental principles of law in the requested Member State.

2. The requested Member State shall execute the request for assistance as soon as possible, taking as full account as possible of the procedural deadlines and other deadlines indicated by the requesting Member State. The requesting Member State shall explain the reasons for the deadline.

3. If the request cannot, or cannot fully, be executed in accordance with the requirements set by the requesting Member State, the authorities of the requested Member State shall promptly inform the authorities of the requesting Member State and indicate the conditions under which it might be possible to execute the request. The authorities of the requesting and the requested Member State may subsequently agree on further action to be taken concerning the request, where necessary by making such action subject to the fulfilment of those conditions.

4. If it is foreseeable that the deadline set by the requesting Member State for executing its request cannot be met, and if the reasons referred to in paragraph 2, second sentence, indicate explicitly that any delay will lead to substantial impairment of the proceedings being conducted in the requesting Member State, the authorities of the requested Member State shall promptly indicate the estimated time needed for execution of the request. The authorities of the requesting Member State shall promptly indicate whether the request is to be upheld nonetheless. The authorities of the requesting and requested Member States may subsequently agree on further action to be taken concerning the request.

Article 5 - Sending and service of procedural documents

1. Each Member State shall send procedural documents intended for persons who are in the territory of another Member State to them directly by post.

2. Procedural documents may be sent via the competent authorities of the requested Member State only if:

- (a) the address of the person for whom the document is intended is unknown or uncertain; or
- (b) the relevant procedural law of the requesting Member State requires proof of service of the document on the addressee, other than proof that can be obtained by post; or
- (c) it has not been possible to serve the document by post; or
- (d) the requesting Member State has justified reasons for considering that dispatch by post will be ineffective or is inappropriate.

3. Where there is reason to believe that the addressee does not understand the language in which the document is drawn up, the document, or at least the important passages thereof, must be translated into (one of) the language(s) of the Member State in the territory of which the addressee is staying. If the authority by which the procedural document was issued knows that the addressee understands only some other language, the document, or at least the important passages thereof, must be translated into that other language.

4. All procedural documents shall be accompanied by a report stating that the addressee may obtain information from the authority by which the document was issued or from other authorities in that Member State regarding his or her rights and obligations concerning the document. Paragraph 3 shall also apply to that report.

5. This Article shall not affect the application of Articles 8, 9 and 12 of the European Mutual Assistance Convention and Articles 32, 34 and 35 of the Benelux Treaty.

Article 6 - Transmission of requests for mutual assistance

1. Requests for mutual assistance and spontaneous exchanges of information referred to in Article 7 shall be made in writing, or by any means capable of producing a written record under conditions allowing the receiving Member State to establish authenticity. Such requests shall be made directly between judicial authorities with territorial competence for initiating and executing them, and shall be returned through the same channels unless otherwise specified in this Article.

Any information laid by a Member State with a view to proceedings before the courts of another Member State within the meaning of Article 21 of the European Mutual Assistance Convention and Article 42 of the Benelux Treaty may be the subject of direct communications between the competent judicial authorities.

2. Paragraph 1 shall not prejudice the possibility of requests being sent or returned in specific cases:

- (a) between a central authority of a Member State and a central authority of another Member State; or
- (b) between a judicial authority of one Member State and a central authority of another Member State.

3. Notwithstanding paragraph 1, the United Kingdom and Ireland, respectively, may, when giving the notification provided for in Article 27(2), declare that requests and communications to it, as specified in the declaration, must be sent via its central authority. These Member States may at any time by a further declaration limit the scope of such a declaration for the purpose of giving greater effect to paragraph 1. They shall do so when the provisions on mutual assistance of the Schengen Implementation Convention are put into effect for them. Any Member State may apply the principle of reciprocity in relation to the declarations referred to above.

4. Any request for mutual assistance may, in case of urgency, be made via the International Criminal Police Organisation (Interpol) or any body competent under provisions adopted pursuant to the Treaty on European Union.

5. Where, in respect of requests pursuant to Articles 12, 13 or 14, the competent authority is a judicial authority or a central authority in one Member State and a police or customs authority in the other Member State, requests may be made and answered directly between these authorities. Paragraph 4 shall apply to these contacts.

6. Where, in respect of requests for mutual assistance in relation to proceedings as envisaged in Article 3(1), the competent authority is a judicial authority or a central authority in one Member State and an administrative authority in the other Member State, requests may be made and answered directly between these authorities.

7. Any Member State may declare, when giving the notification provided for in Article 27(2), that it is not bound by the first sentence of paragraph 5 or by paragraph 6 of this Article, or both or that it will apply those provisions only under certain conditions which it shall specify. Such a declaration may be withdrawn or amended at any time.

8. The following requests or communications shall be made through the central authorities of the Member States:

- (a) requests for temporary transfer or transit of persons held in custody as referred to in Article 9 of this Convention, in Article 11 of the European Mutual Assistance Convention and in Article 33 of the Benelux Treaty;
- (b) notices of information from judicial records as referred to in Article 22 of the European Mutual Assistance Convention and Article 43 of the Benelux Treaty. However, requests for copies of convictions and measures as referred to in Article 4 of the Additional Protocol to the European Mutual Assistance Convention may be made directly to the competent authorities.

Article 7 - Spontaneous exchange of information

1. Within the limits of their national law, the competent authorities of the Member States may exchange information, without a request to that effect, relating to criminal offences and the infringements of rules of law referred to in Article 3(1), the punishment or handling of which falls within the competence of the receiving authority at the time the information is provided.

2. The providing authority may, pursuant to its national law, impose conditions on the use of such information by the receiving authority.

3. The receiving authority shall be bound by those conditions.

13.1.7 Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime

Article 4 - Processing of requests for mutual assistance

Member States shall take the necessary steps to ensure that all requests from other Member States which relate to asset identification, tracing, freezing or seizing and confiscation are processed with the same priority as is given to such measures in domestic proceedings.

13.1.8 The protocol to the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU

Article 1 - Request for information on bank accounts

1. Each Member State shall, under the conditions set out in this Article, take the measures necessary to determine, in answer to a request sent by another Member State, whether a natural or legal person that is the subject of a criminal investigation holds or controls one or more accounts, of whatever nature, in any bank located in its territory and, if so, provide all the details of the identified accounts.

The information shall also, if requested and to the extent that it can be provided within a reasonable time, include accounts for which the person that is the subject of the proceedings has powers of attorney.

2. The obligation set out in this Article shall apply only to the extent that the information is in the possession of the bank keeping the account.

3. The obligation set out in this Article shall apply only if the investigation concerns

- an offence punishable by a penalty involving deprivation of liberty or a detention order of a maximum period of at least four years in the requesting State and at least two years in the requested State, or

- an offence referred to in Article 2 of the 1995 Convention on the establishment of a European Police Office (Europol Convention), or in the Annex to that Convention, as amended, or

- to the extent that it may not be covered by the Europol Convention, an offence referred to in the 1995 Convention on the protection of the European Communities' financial interests, the 1996 Protocol thereto, or the 1997 Second Protocol thereto.

4. The authority making the request shall, in the request:

- state why it considers that the requested information is likely to be of substantial value for the purpose of the investigation into the offence;

- state on what grounds it presumes that banks in the requested Member State hold the account and, to the extent available, which banks may be involved;

- include any information available which may facilitate the execution of the request.

5. Member States may make the execution of a request according to this Article dependent on the same conditions as they apply in respect of requests for search and seizure.

6. The Council may decide, pursuant to Article 34(2) (c) of the Treaty of European Union, to extend the scope of paragraph 3.

Article 2 - Requests for information on banking transactions

1. On request by the requesting State, the requested State shall provide the particulars of specified bank accounts and of banking operations which have been carried out during a specified period through one or more accounts specified in the request, including the particulars of any sending or recipient account.

2. The obligation set out in this Article shall apply only to the extent that the information is in the possession of the bank holding the account.

3. The requesting Member State shall in its request indicate why it considers the requested information relevant for the purpose of the investigation into the offence.

4. Member States may make the execution of a request according to this Article dependent on the same conditions as they apply in respect of requests for search and seizure.

Article 3 - Requests for the monitoring of banking transactions

1. Each Member State shall undertake to ensure that, at the request of another Member State, it is able to monitor, during a specified period, the banking operations that are being carried out through one or more accounts specified in the request and communicate the results thereof to the requesting Member State.

2. The requesting Member State shall in its request indicate why it considers the requested information relevant for the purpose of the investigation into the offence.

3. The decision to monitor shall be taken in each individual case by the competent authorities of the requested Member State, with due regard for the national law of that Member State.

4. The practical details regarding the monitoring shall be agreed between the competent authorities of the requesting and requested Member States.

Article 4 - Confidentiality

Each Member State shall take the necessary measures to ensure that banks do not disclose to the bank customer concerned or to other third persons that information has been transmitted to the requesting State in accordance with Articles 1, 2 or 3 or that an investigation is being carried out.

Article 5 - Obligation to inform

If the competent authority of the requested Member State in the course of the execution of a request for mutual assistance considers that it may be appropriate to undertake investigations not initially foreseen, or which could not be

specified when the request was made, it shall immediately inform the requesting authority accordingly in order to enable it to take further action.

Article 6 - Additional requests for mutual assistance

1. Where the competent authority of the requesting Member State makes a request for mutual assistance which is additional to an earlier request, it shall not be required to provide information already provided in the initial request. The additional request shall contain information necessary for the purpose of identifying the initial request.
2. Where, in accordance with the provisions in force, the competent authority which has made a request for mutual assistance participates in the execution of the request in the requested Member State, it may, without prejudice to Article 6(3) of the 2000 Mutual Assistance Convention, make an additional request directly to the competent authority of the requested Member State while present in that State.

Article 7 - Banking secrecy

A Member State shall not invoke banking secrecy as a reason for refusing any cooperation regarding a request for mutual assistance from another Member State.

Article 8 - Fiscal offences

1. Mutual assistance may not be refused solely on the ground that the request concerns an offence which the requested Member State considers a fiscal offence.
2. If a Member State has made the execution of a request for search and seizure dependent on the condition that the offence giving rise to the request is also punishable under its law, this condition shall be fulfilled, with regard to offences referred to in paragraph 1, if the offence corresponds to an offence of the same nature under its law. The request may not be refused on the ground that the law of the requested Member State does not impose the same kind of tax or duty or does not contain a tax, duty, customs and exchange regulation of the same kind as the law of the requesting Member State.
3. Article 50 of the Schengen Implementation Convention is hereby repealed.

Article 9 - Political offences

1. For the purposes of mutual legal assistance between Member States, no offence may be regarded by the requested Member State as a political offence, an offence connected with a political offence or an offence inspired by political motives.
2. Each Member State may, when giving the notification referred to in Article 13(2), declare that it will apply paragraph 1 only in relation to
 - (a) the offences referred to in Articles 1 and 2 of the European Convention on the Suppression of Terrorism of 27 January 1977; and
 - (b) offences of conspiracy or association - which correspond to the description of behaviour referred to in Article 3(4) of the Convention of 27 September 1996 relating to extradition between the Member States of the European Union - to commit one or more of the offences referred to in Articles 1 and 2 of the European Convention on the Suppression of Terrorism.
3. Reservations made pursuant to Article 13 of the European Convention on the Suppression of Terrorism shall not apply to mutual legal assistance between Member States.

13.2 Asset recovery

13.2.1 FATF 40 Recommendations

Recommendation 38

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

Interpretative Note to Recommendation 38

1. Countries should consider establishing an asset forfeiture fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes. Countries should take such measures as may be necessary to enable them to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions.

2. With regard to requests for cooperation made on the basis of non-conviction based confiscation proceedings, countries need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.

13.2.2 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 5

4. (a) Following a request made pursuant to this article by another Party having jurisdiction over an offence established in accordance with article 3, paragraph 1, the Party in whose territory proceeds, property, instrumentalities or any other things referred to in paragraph 1 of this article are situated shall:

(i) Submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such order is granted, give effect to it; or

(ii) Submit to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by the requesting Party in accordance with paragraph 1 of this article, in so far as it relates to proceeds, property, instrumentalities or any other things referred to in paragraph 1 situated in the territory of the requested Party.

(b) Following a request made pursuant to this article by another Party having jurisdiction over an offence established in accordance with article 3, paragraph 1, the requested Party shall take measures to identify, trace, and freeze or seize proceeds, property, instrumentalities or any other things referred to in paragraph 1 of this article for the purpose of eventual confiscation to be ordered either by the requesting Party or, pursuant to a request under subparagraph (a) of this paragraph, by the requested Party.

(c) The decisions or actions provided for in subparagraphs (a) and (b) of this paragraph shall be taken by the requested Party, in accordance with and subject to the provisions of its domestic law and its procedural rules or any bilateral or multilateral treaty, agreement or arrangement to which it may be bound in relation to the requesting Party.

(d) The provisions of article 7, paragraphs 6 to 19 are applicable *mutatis mutandis*. In addition to the information specified in article 7, paragraph 10, requests made pursuant to this article shall contain the following:

(i) In the case of a request pertaining to subparagraph (a)(i) of this paragraph, a description of the property to be confiscated and a statement of the facts relied upon by the requesting Party sufficient to enable the requested Party to seek the order under its domestic law;

(ii) In the case of a request pertaining to subparagraph (a)(ii), a legally admissible copy of an order of confiscation issued by the requesting Party upon which the request is based, a statement of the facts and information as to the extent to which the execution of the order is requested;

(iii) In the case of a request pertaining to subparagraph (b), a statement of the facts relied upon by the requesting Party and a description of the actions requested.

(e) Each Party shall furnish to the Secretary-General the text of any of its laws and regulations which give effect to this paragraph and the text of any subsequent changes to such laws and regulations.

(f) If a Party elects to make the taking of the measures referred to in subparagraphs (a) and (b) of this paragraph conditional on the existence of a relevant treaty, that Party shall consider this Convention as the necessary and sufficient treaty basis.

(g) The Parties shall seek to conclude bilateral and multilateral treaties, agreements or arrangements to enhance the effectiveness of international co-operation pursuant to this article.

5. (a) Proceeds or property confiscated by a Party pursuant to paragraph 1 or paragraph 4 of this article shall be disposed of by that Party according to its domestic law and administrative procedures.

(b) When acting on the request of another Party in accordance with this article, a Party may give special consideration to concluding agreements on:

(i) Contributing the value of such proceeds and property, or funds derived from the sale of such proceeds or property, or a substantial part thereof, to intergovernmental bodies specializing in the fight against illicit traffic in and abuse of narcotic drugs and psychotropic substances;

(ii) Sharing with other Parties, on a regular or case-by-case basis, such proceeds or property, or funds derived from the sale of such proceeds or property, in accordance with its domestic law, administrative procedures or bilateral or multilateral agreements entered into for this purpose.

13.2.3 2000 UN Convention against Transnational Organized Crime

Article 13 - International cooperation for purposes of confiscation

1. A State Party that has received a request from another State Party having jurisdiction over an offence covered by this Convention for confiscation of proceeds of crime, property, equipment or other instrumentalities referred to in article 12, paragraph 1, of this Convention situated in its territory shall, to the greatest extent possible within its domestic legal system:

(a) Submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such an order is granted, give effect to it; or

(b) Submit to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by a court in the territory of the requesting State Party in accordance with article 12, paragraph 1, of this Convention insofar as it relates to proceeds of crime, property, equipment or other instrumentalities referred to in article 12, paragraph 1, situated in the territory of the requested State Party.

2. Following a request made by another State Party having jurisdiction over an offence covered by this Convention, the requested State Party shall take measures to identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in article 12, paragraph 1, of this Convention for the purpose of eventual confiscation to be ordered either by the requesting State Party or, pursuant to a request under paragraph 1 of this article, by the requested State Party.

3. The provisions of article 18 of this Convention are applicable, mutatis mutandis, to this article. In addition to the information specified in article 18, paragraph 15, requests made pursuant to this article shall contain:

(a) In the case of a request pertaining to paragraph 1 (a) of this article, a description of the property to be confiscated and a statement of the facts relied upon by the requesting State Party sufficient to enable the requested State Party to seek the order under its domestic law;

(b) In the case of a request pertaining to paragraph 1 (b) of this article, a legally admissible copy of an order of confiscation upon which the request is based issued by the requesting State Party, a statement of the facts and information as to the extent to which execution of the order is requested;

(c) In the case of a request pertaining to paragraph 2 of this article, a statement of the facts relied upon by the requesting State Party and a description of the actions requested.

4. The decisions or actions provided for in paragraphs 1 and 2 of this article shall be taken by the requested State Party in accordance with and subject to the provisions of its domestic law and its procedural rules or any bilateral or multilateral treaty, agreement or arrangement to which it may be bound in relation to the requesting State Party.

5. Each State Party shall furnish copies of its laws and regulations that give effect to this article and of any subsequent changes to such laws and regulations or a description thereof to the Secretary-General of the United Nations.

6. If a State Party elects to make the taking of the measures referred to in paragraphs 1 and 2 of this article conditional on the existence of a relevant treaty, that State Party shall consider this Convention the necessary and sufficient treaty basis.

7. Cooperation under this article may be refused by a State Party if the offence to which the request relates is not an offence covered by this Convention.

8. The provisions of this article shall not be construed to prejudice the rights of bona fide third parties.

9. States Parties shall consider concluding bilateral or multilateral treaties, agreements or arrangements to enhance the effectiveness of international cooperation undertaken pursuant to this article.

Article 14 - Disposal of confiscated proceeds of crime or property

1. Proceeds of crime or property confiscated by a State Party pursuant to articles 12 or 13, paragraph 1, of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on the request made by another State Party in accordance with article 13 of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners.

3. When acting on the request made by another State Party in accordance with articles 12 and 13 of this Convention, a State Party may give special consideration to concluding agreements or arrangements on:

(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with article 30, paragraph 2 (c), of this Convention and to intergovernmental bodies specializing in the fight against organized crime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

13.2.4 2003 UN Convention against Corruption

Article 51 - General provision

The return of assets pursuant to this chapter is a fundamental principle of this Convention, and States Parties shall afford one another the widest measure of cooperation and assistance in this regard.

Article 52 - Prevention and detection of transfers of proceeds of crime

1. Without prejudice to article 14 of this Convention, each State Party shall take such measures as may be necessary, in accordance with its domestic law, to require financial institutions within its jurisdiction to verify the identity of customers, to take reasonable steps to determine the identity of beneficial owners of funds deposited into high-value accounts and to conduct enhanced scrutiny of accounts sought or maintained by or on behalf of individuals who are, or have been, entrusted with prominent public functions and their family members and close associates. Such enhanced scrutiny shall be reasonably designed to detect suspicious transactions for the purpose of reporting to competent

authorities and should not be so construed as to discourage or prohibit financial institutions from doing business with any legitimate customer.

2. In order to facilitate implementation of the measures provided for in paragraph 1 of this article, each State Party, in accordance with its domestic law and inspired by relevant initiatives of regional, interregional and multilateral organizations against money-laundering, shall:

(a) Issue advisories regarding the types of natural or legal person to whose accounts financial institutions within its jurisdiction will be expected to apply enhanced scrutiny, the types of accounts and transactions to which to pay particular attention and appropriate account-opening, maintenance and record-keeping measures to take concerning such accounts; and

(b) Where appropriate, notify financial institutions within its jurisdiction, at the request of another State Party or on its own initiative, of the identity of particular natural or legal persons to whose accounts such institutions will be expected to apply enhanced scrutiny, in addition to those whom the financial institutions may otherwise identify.

3. In the context of paragraph 2 (a) of this article, each State Party shall implement measures to ensure that its financial institutions maintain adequate records, over an appropriate period of time, of accounts and transactions involving the persons mentioned in paragraph 1 of this article, which should, as a minimum, contain information relating to the identity of the customer as well as, as far as possible, of the beneficial owner.

4. With the aim of preventing and detecting transfers of proceeds of offences established in accordance with this Convention, each State Party shall implement appropriate and effective measures to prevent, with the help of its regulatory and oversight bodies, the establishment of banks that have no physical presence and that are not affiliated with a regulated financial group. Moreover, States Parties may consider requiring their financial institutions to refuse to enter into or continue a correspondent banking relationship with such institutions and to guard against establishing relations with foreign financial institutions that permit their accounts to be used by banks that have no physical presence and that are not affiliated with a regulated financial group.

5. Each State Party shall consider establishing, in accordance with its domestic law, effective financial disclosure systems for appropriate public officials and shall provide for appropriate sanctions for non-compliance. Each State Party shall also consider taking such measures as may be necessary to permit its competent authorities to share that information with the competent authorities in other States Parties when necessary to investigate, claim and recover proceeds of offences established in accordance with this Convention.

6. Each State Party shall consider taking such measures as may be necessary, in accordance with its domestic law, to require appropriate public officials having an interest in or signature or other authority over a financial account in a foreign country to report that relationship to appropriate authorities and to maintain appropriate records related to such accounts. Such measures shall also provide for appropriate sanctions for non-compliance.

Article 53 - Measures for direct recovery of property

Each State Party shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit another State Party to initiate civil action in its courts to establish title to or ownership of property acquired through the commission of an offence established in accordance with this Convention;

(b) Take such measures as may be necessary to permit its courts to order those who have committed offences established in accordance with this Convention to pay compensation or damages to another State Party that has been harmed by such offences; and

(c) Take such measures as may be necessary to permit its courts or competent authorities, when having to decide on confiscation, to recognize another State Party's claim as a legitimate owner of property acquired through the commission of an offence established in accordance with this Convention.

Article 54 - Mechanisms for recovery of property through international cooperation in confiscation

1. Each State Party, in order to provide mutual legal assistance pursuant to article 55 of this Convention with respect to property acquired through or involved in the commission of an offence established in accordance with this Convention, shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit its competent authorities to give effect to an order of confiscation issued by a court of another State Party;

(b) Take such measures as may be necessary to permit its competent authorities, where they have jurisdiction, to order the confiscation of such property of foreign origin by adjudication of an offence of money-laundering or such other offence as may be within its jurisdiction or by other procedures authorized under its domestic law; and

(c) Consider taking such measures as may be necessary to allow confiscation of such property without a criminal conviction in cases in which the offender cannot be prosecuted by reason of death, flight or absence or in other appropriate cases.

2. Each State Party, in order to provide mutual legal assistance upon a request made pursuant to paragraph 2 of article 55 of this Convention, shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a freezing or seizure order issued by a court or competent authority of a requesting State Party that provides a reasonable basis for the requested State Party to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for purposes of paragraph 1 (a) of this article;

- (b) Take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a request that provides a reasonable basis for the requested State Party to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for purposes of paragraph 1 (a) of this article; and
- (c) Consider taking additional measures to permit its competent authorities to preserve property for confiscation, such as on the basis of a foreign arrest or criminal charge related to the acquisition of such property.

Article 55 - International cooperation for purposes of confiscation

1. A State Party that has received a request from another State Party having jurisdiction over an offence established in accordance with this Convention for confiscation of proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention situated in its territory shall, to the greatest extent possible within its domestic legal system:

(a) Submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such an order is granted, give effect to it; or

(b) Submit to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by a court in the territory of the requesting State Party in accordance with articles 31, paragraph 1, and 54, paragraph 1 (a), of this Convention insofar as it relates to proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, situated in the territory of the requested State Party.

2. Following a request made by another State Party having jurisdiction over an offence established in accordance with this Convention, the requested State Party shall take measures to identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention for the purpose of eventual confiscation to be ordered either by the requesting State Party or, pursuant to a request under paragraph 1 of this article, by the requested State Party.

3. The provisions of article 46 of this Convention are applicable, mutates mutandis, to this article. In addition to the information specified in article 46, paragraph 15, requests made pursuant to this article shall contain:

(a) In the case of a request pertaining to paragraph 1 (a) of this article, a description of the property to be confiscated, including, to the extent possible, the location and, where relevant, the estimated value of the property and a statement of the facts relied upon by the requesting State Party sufficient to enable the requested State Party to seek the order under its domestic law;

(b) In the case of a request pertaining to paragraph 1 (b) of this article, a legally admissible copy of an order of confiscation upon which the request is based issued by the requesting State Party, a statement of the facts and information as to the extent to which execution of the order is requested, a statement specifying the measures taken by the requesting State Party to provide adequate notification to bona fide third parties and to ensure due process and a statement that the confiscation order is final;

(c) In the case of a request pertaining to paragraph 2 of this article, a statement of the facts relied upon by the requesting State Party and a description of the actions requested and, where available, a legally admissible copy of an order on which the request is based.

4. The decisions or actions provided for in paragraphs 1 and 2 of this article shall be taken by the requested State Party in accordance with and subject to the provisions of its domestic law and its procedural rules or any bilateral or multilateral agreement or arrangement to which it may be bound in relation to the requesting State Party.

5. Each State Party shall furnish copies of its laws and regulations that give effect to this article and of any subsequent changes to such laws and regulations or a description thereof to the Secretary-General of the United Nations.

6. If a State Party elects to make the taking of the measures referred to in paragraphs 1 and 2 of this article conditional on the existence of a relevant treaty, that State Party shall consider this Convention the necessary and sufficient treaty basis.

7. Cooperation under this article may also be refused or provisional measures lifted if the requested State Party does not receive sufficient and timely evidence or if the property is of a *de minimis* value.

8. Before lifting any provisional measure taken pursuant to this article, the requested State Party shall, wherever possible, give the requesting State Party an opportunity to present its reasons in favour of continuing the measure.

9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

Article 56 - Special cooperation

Without prejudice to its domestic law, each State Party shall endeavour to take measures to permit it to forward, without prejudice to its own investigations, prosecutions or judicial proceedings, information on proceeds of offences established in accordance with this Convention to another State Party without prior request, when it considers that the disclosure of such information might assist the receiving State Party in initiating or carrying out investigations, prosecutions or judicial proceedings or might lead to a request by that State Party under this chapter of the Convention.

Article 57 - Return and disposal of assets

1. Property confiscated by a State Party pursuant to article 31 or 55 of this Convention shall be disposed of, including by return to its prior legitimate owners, pursuant to paragraph 3 of this article, by that State Party in accordance with the provisions of this Convention and its domestic law.

2. Each State Party shall adopt such legislative and other measures, in accordance with the fundamental principles of its domestic law, as may be necessary to enable its competent authorities to return confiscated property, when acting on the request made by another State Party, in accordance with this Convention, taking into account the rights of bona fide third parties.

3. In accordance with articles 46 and 55 of this Convention and paragraphs 1 and 2 of this article, the requested State Party shall:

(a) In the case of embezzlement of public funds or of laundering of embezzled public funds as referred to in articles 17 and 23 of this Convention, when confiscation was executed in accordance with article 55 and on the basis of a final judgement in the requesting State Party, a requirement that can be waived by the requested State Party, return the confiscated property to the requesting State Party;

(b) In the case of proceeds of any other offence covered by this Convention, when the confiscation was executed in accordance with article 55 of this Convention and on the basis of a final judgement in the requesting State Party, a requirement that can be waived by the requested State Party, return the confiscated property to the requesting State Party, when the requesting State Party reasonably establishes its prior ownership of such confiscated property to the requested State Party or when the requested State Party recognizes damage to the requesting State Party as a basis for returning the confiscated property;

(c) In all other cases, give priority consideration to returning confiscated property to the requesting State Party, returning such property to its prior legitimate owners or compensating the victims of the crime.

4. Where appropriate, unless States Parties decide otherwise, the requested State Party may deduct reasonable expenses incurred in investigations, prosecutions or judicial proceedings leading to the return or disposition of confiscated property pursuant to this article.

5. Where appropriate, States Parties may also give special consideration to concluding agreements or mutually acceptable arrangements, on a case-by-case basis, for the final disposal of confiscated property.

Article 59- Bilateral and multilateral agreements and arrangements

States Parties shall consider concluding bilateral or multilateral agreements or arrangements to enhance the effectiveness of international cooperation undertaken pursuant to this chapter of the Convention.

13.2.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 21 – Obligation to take provisional measures

1 At the request of another Party which has instituted criminal proceedings or proceedings for the purpose of confiscation, a Party shall take the necessary provisional measures, such as freezing or seizing, to prevent any dealing in, transfer or disposal of property which, at a later stage, may be the subject of a request for confiscation or which might be such as to satisfy the request.

2 A Party which has received a request for confiscation pursuant to Article 23 shall, if so requested, take the measures mentioned in paragraph 1 of this article in respect of any property which is the subject of the request or which might be such as to satisfy the request.

Article 22 – Execution of provisional measures

1 After the execution of the provisional measures requested in conformity with paragraph 1 of Article 21, the requesting Party shall provide spontaneously and as soon as possible to the requested Party all information which may question or modify the extent of these measures. The requesting Party shall also provide without delays all complementary information requested by the requested Party and which is necessary for the implementation of and the follow up to the provisional measures.

2 Before lifting any provisional measure taken pursuant to this article, the requested Party shall, wherever possible, give the requesting Party an opportunity to present its reasons in favour of continuing the measure.

Article 23 – Obligation to confiscate

1 A Party, which has received a request made by another Party for confiscation concerning instrumentalities or proceeds, situated in its territory, shall:

a enforce a confiscation order made by a court of a requesting Party in relation to such instrumentalities or proceeds; or

b submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such order is granted, enforce it.

2 For the purposes of applying paragraph 1.b of this article, any Party shall whenever necessary have competence to institute confiscation proceedings under its own law.

3 The provisions of paragraph 1 of this article shall also apply to confiscation consisting in a requirement to pay a sum of money corresponding to the value of proceeds, if property on which the confiscation can be enforced is located in the requested Party. In such cases, when enforcing confiscation pursuant to paragraph 1, the requested Party shall, if payment is not obtained, realise the claim on any property available for that purpose.

4 If a request for confiscation concerns a specific item of property, the Parties may agree that the requested Party may enforce the confiscation in the form of a requirement to pay a sum of money corresponding to the value of the property.

5. The Parties shall co-operate to the widest extent possible under their domestic law with those Parties which request the execution of measures equivalent to confiscation leading to the deprivation of property, which are not criminal sanctions, in so far as such measures are ordered by a judicial authority of the requesting Party in relation to a criminal offence, provided that it has been established that the property constitutes proceeds or other property in the meaning of Article 5 of this Convention.

Article 24 – Execution of confiscation

1 The procedures for obtaining and enforcing the confiscation under Article 23 shall be governed by the law of the requested Party.

2 The requested Party shall be bound by the findings as to the facts in so far as they are stated in a conviction or judicial decision of the requesting Party or in so far as such conviction or judicial decision is implicitly based on them.

3 Each State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that paragraph 2 of this article applies only subject to its constitutional principles and the basic concepts of its legal system.

4 If the confiscation consists in the requirement to pay a sum of money, the competent authority of the requested Party shall convert the amount thereof into the currency of that Party at the rate of exchange ruling at the time when the decision to enforce the confiscation is taken.

5 In the case of Article 23, paragraph 1.a, the requesting Party alone shall have the right to decide on any application for review of the confiscation order.

Article 25 – Confiscated property

1 Property confiscated by a Party pursuant to Articles 23 and 24 of this Convention, shall be disposed of by that Party in accordance with its domestic law and administrative procedures.

2 When acting on the request made by another Party in accordance with Articles 23 and 24 of this Convention, Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated property to the requesting Party so that it can give compensation to the victims of the crime or return such property to their legitimate owners.

3 When acting on the request made by another Party in accordance with Articles 23 and 24 of this Convention, a Party may give special consideration to concluding agreements or arrangements on sharing with other Parties, on a regular or case-by-case basis, such property, in accordance with its domestic law or administrative procedures.

Article 26 – Right of enforcement and maximum amount of confiscation

1 A request for confiscation made under Articles 23 and 24 does not affect the right of the requesting Party to enforce itself the confiscation order.

2 Nothing in this Convention shall be so interpreted as to permit the total value of the confiscation to exceed the amount of the sum of money specified in the confiscation order. If a Party finds that this might occur, the Parties concerned shall enter into consultations to avoid such an effect.

Article 27 – Imprisonment in default

The requested Party shall not impose imprisonment in default or any other measure restricting the liberty of a person as a result of a request under Article 23, if the requesting Party has so specified in the request.

Article 28 – Grounds for refusal

1 Co-operation under this chapter may be refused if:

- a the action sought would be contrary to the fundamental principles of the legal system of the requested Party; or
- b the execution of the request is likely to prejudice the sovereignty, security, ordre public or other essential interests of the requested Party; or
- c in the opinion of the requested Party, the importance of the case to which the request relates does not justify the taking of the action sought; or
- d the offence to which the request relates is a fiscal offence, with the exception of the financing of terrorism;
- e the offence to which the request relates is a political offence, with the exception of the financing of terrorism; or
- f the requested Party considers that compliance with the action sought would be contrary to the principle of "*ne bis in idem*"; or
- g the offence to which the request relates would not be an offence under the law of the requested Party if committed within its jurisdiction. However, this ground for refusal applies to co-operation under Section 2 only in so far as the assistance sought involves coercive action. Where dual criminality is required for co-operation under this chapter, that requirement shall be deemed to be satisfied regardless of whether both Parties place the offence within the same category of offences or denominate the offence by the same terminology, provided that both Parties criminalise the conduct underlying the offence.

2 Co-operation under Section 2, in so far as the assistance sought involves coercive action, and under Section 3 of this chapter, may also be refused if the measures sought could not be taken under the domestic law of the requested Party for the purposes of investigations or proceedings, had it been a similar domestic case.

3 Where the law of the requested Party so requires, co-operation under Section 2, in so far as the assistance sought involves coercive action, and under Section 3 of this chapter may also be refused if the measures sought or any other measures having similar effects would not be permitted under the law of the requesting Party, or, as regards the competent authorities of the requesting Party, if the request is not authorised by either a judge or another judicial authority, including public prosecutors, any of these authorities acting in relation to criminal offences.

4 Co-operation under Section 4 of this chapter may also be refused if:

a under the law of the requested Party confiscation is not provided for in respect of the type of offence to which the request relates; or

b without prejudice to the obligation pursuant to Article 23, paragraph 3, it would be contrary to the principles of the domestic law of the requested Party concerning the limits of confiscation in respect of the relationship between an offence and:

i an economic advantage that might be qualified as its proceeds; or

ii property that might be qualified as its instrumentalities; or

c under the law of the requested Party confiscation may no longer be imposed or enforced because of the lapse of time; or

d without prejudice to Article 23, paragraph 5, the request does not relate to a previous conviction, or a decision of a judicial nature or a statement in such a decision that an offence or several offences have been committed, on the basis of which the confiscation has been ordered or is sought; or

e confiscation is either not enforceable in the requesting Party, or it is still subject to ordinary means of appeal; or

f the request relates to a confiscation order resulting from a decision rendered in absentia of the person against whom the order was issued and, in the opinion of the requested Party, the proceedings conducted by the requesting Party leading to such decision did not satisfy the minimum rights of defence recognised as due to everyone against whom a criminal charge is made.

5 For the purpose of paragraph 4.f of this article a decision is not considered to have been rendered *in absentia* if:

a it has been confirmed or pronounced after opposition by the person concerned; or

b it has been rendered on appeal, provided that the appeal was lodged by the person concerned.

6 When considering, for the purposes of paragraph 4.f of this article if the minimum rights of defence have been satisfied, the requested Party shall take into account the fact that the person concerned has deliberately sought to evade justice or the fact that that person, having had the possibility of lodging a legal remedy against the decision made *in absentia*, elected not to do so. The same will apply when the person concerned, having been duly served with the summons to appear, elected not to do so nor to ask for adjournment.

7 A Party shall not invoke bank secrecy as a ground to refuse any co-operation under this chapter. Where its domestic law so requires, a Party may require that a request for co-operation which would involve the lifting of bank secrecy be authorised by either a judge or another judicial authority, including public prosecutors, any of these authorities acting in relation to criminal offences.

8 Without prejudice to the ground for refusal provided for in paragraph 1.a of this article:

a the fact that the person under investigation or subjected to a confiscation order by the authorities of the requesting Party is a legal person shall not be invoked by the requested Party as an obstacle to affording any co-operation under this chapter;

b the fact that the natural person against whom an order of confiscation of proceeds has been issued has died or the fact that a legal person against whom an order of confiscation of proceeds has been issued has subsequently been dissolved shall not be invoked as an obstacle to render assistance in accordance with Article 23, paragraph 1.a;

c the fact that the person under investigation or subjected to a confiscation order by the authorities of the requesting Party is mentioned in the request both as the author of the underlying criminal offence and of the offence of money laundering, in accordance with Article 9.2.b of this Convention, shall not be invoked by the requested Party as an obstacle to affording any co-operation under this chapter.

Article 29 – Postponement

The requested Party may postpone action on a request if such action would prejudice investigations or proceedings by its authorities.

Article 30 – Partial or conditional granting of a request

Before refusing or postponing co-operation under this chapter, the requested Party shall, where appropriate after having consulted the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

Article 31 – Notification of documents

1 The Parties shall afford each other the widest measure of mutual assistance in the serving of judicial documents to persons affected by provisional measures and confiscation.

2 Nothing in this article is intended to interfere with:

- a the possibility of sending judicial documents, by postal channels, directly to persons abroad;
 - b the possibility for judicial officers, officials or other competent authorities of the Party of origin to effect service of judicial documents directly through the consular authorities of that Party or through judicial officers, officials or other competent authorities of the Party of destination, unless the Party of destination makes a declaration to the contrary to the Secretary General of the Council of Europe at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.
- 3 When serving judicial documents to persons abroad affected by provisional measures or confiscation orders issued in the sending Party, this Party shall indicate what legal remedies are available under its law to such persons.

Article 32 – Recognition of foreign decisions

- 1 When dealing with a request for co-operation under Sections 3 and 4, the requested Party shall recognise any judicial decision taken in the requesting Party regarding rights claimed by third parties.
- 2 Recognition may be refused if:
- a third parties did not have adequate opportunity to assert their rights; or
 - b the decision is incompatible with a decision already taken in the requested Party on the same matter; or
 - c it is incompatible with the ordre public of the requested Party; or
 - d the decision was taken contrary to provisions on exclusive jurisdiction provided for by the law of the requested Party.

13.3 Jurisdiction and Extradition

13.3.1 FATF Recommendations

Recommendation 39

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. 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. In particular, countries should:

- (a) ensure money laundering and terrorist financing are extraditable offences;
- (b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;
- (c) not place unreasonable or unduly restrictive conditions on the execution of requests; and
- (d) ensure they have an adequate legal framework for extradition.

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.

Where dual criminality is required for 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.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

13.3.2 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 4

1. Each Party:

(a) Shall take such measures as may be necessary to establish its jurisdiction over the offences it has established in accordance with article 3, paragraph 1, when:

- (i) The offence is committed in its territory;
- (ii) The offence is committed on board a vessel flying its flag or an aircraft which is registered under its laws at the time the offence is committed;

(b) May take such measures as may be necessary to establish its jurisdiction over the offences it has established in accordance with article 3, paragraph 1, when:

- (i) The offence is committed by one of its nationals or by a person who has his habitual residence in its territory;
- (ii) The offence is committed on board a vessel concerning which that Party has been authorized to take appropriate action pursuant to article 17, provided that such jurisdiction shall be exercised only on the basis of agreements or arrangements referred to in paragraphs 4 and 9 of that article;
- (iii) The offence is one of those established in accordance with article 3, paragraph 1, subparagraph (c)(iv), and is committed outside its territory with a view to the commission, within its territory, of an offence established in accordance with article 3, paragraph 1.

2. Each Party:

(a) Shall also take such measures as may be necessary to establish its jurisdiction over the offences it has established in accordance with article 3, paragraph 1, when the alleged offender is present in its territory and it does not extradite him to another Party on the ground:

- (i) That the offence has been committed in its territory or on board a vessel flying its flag or an aircraft which was registered under its law at the time the offence was committed; or
- (ii) That the offence has been committed by one of its nationals;

(b) May also take such measures as may be necessary to establish its jurisdiction over the offences it has established in accordance with article 3, paragraph 1, when the alleged offender is present in its territory and it does not extradite him to another Party.

3. This Convention does not exclude the exercise of any criminal jurisdiction established by a Party in accordance with its domestic law.

Article 6

1. This article shall apply to the offences established by the Parties in accordance with article 3, paragraph 1.
2. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between Parties. The Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.
3. If a Party which makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it has no extradition treaty, it may consider this Convention as the legal basis for extradition in respect of any offence to which this article applies. The Parties which require detailed legislation in order to use this Convention as a legal basis for extradition shall consider enacting such legislation as may be necessary.
4. The Parties which do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.
5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds upon which the requested Party may refuse extradition.
6. In considering requests received pursuant to this article, the requested State may refuse to comply with such requests where there are substantial grounds leading its judicial or other competent authorities to believe that compliance would facilitate the prosecution or punishment of any person on account of his race, religion, nationality or political opinions, or would cause prejudice for any of those reasons to any person affected by the request.
7. The Parties shall endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.
8. Subject to the provisions of its domestic law and its extradition treaties, the requested Party may, upon being satisfied that the circumstances so warrant and are urgent, and at the request of the requesting Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his presence at extradition proceedings.
9. Without prejudice to the exercise of any criminal jurisdiction established in accordance with its domestic law, a Party in whose territory an alleged offender is found shall:
 - (a) If it does not extradite him in respect of an offence established in accordance with article 3, paragraph 1, on the grounds set forth in article 4, paragraph 2, subparagraph (a), submit the case to its competent authorities for the purpose of prosecution, unless otherwise agreed with the requesting Party;
 - (b) If it does not extradite him in respect of such an offence and has established its jurisdiction in relation to that offence in accordance with article 4, paragraph 2, subparagraph (b), submit the case to its competent authorities for the purpose of prosecution, unless otherwise requested by the requesting Party for the purposes of preserving its legitimate jurisdiction.
10. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested Party, the requested Party shall, if its law so permits and in conformity with the requirements of such law, upon application of the requesting Party, consider the enforcement of the sentence which has been imposed under the law of the requesting Party, or the remainder thereof.
11. The Parties shall seek to conclude bilateral and multilateral agreements to carry out or to enhance the effectiveness of extradition.
12. The Parties may consider entering into bilateral or multilateral agreements, whether *ad hoc* or general, on the transfer to their country of persons sentenced to imprisonment and other forms of deprivation of liberty for offences to which this article applies, in order that they may complete their sentences there.

13.3.3 2000 UN Convention against Transnational Organized Crime

Article 11 - Prosecution, adjudication and sanctions

1. Each State Party shall make the commission of an offence established in accordance with articles 5, 6, 8 and 23 of this Convention liable to sanctions that take into account the gravity of that offence.
2. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by this Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.
3. In the case of offences established in accordance with articles 5, 6, 8 and 23 of this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.
4. Each State Party shall ensure that its courts or other competent authorities bear in mind the grave nature of the offences covered by this Convention when considering the eventuality of early release or parole of persons convicted of such offences.

5. Each State Party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence covered by this Convention and a longer period where the alleged offender has evaded the administration of justice.
6. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.

Article 15 - Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with articles 5, 6, 8 and 23 of this Convention when:
 - (a) The offence is committed in the territory of that State Party; or
 - (b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.
2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:
 - (a) The offence is committed against a national of that State Party;
 - (b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory; or
 - (c) The offence is:
 - (i) One of those established in accordance with article 5, paragraph 1, of this Convention and is committed outside its territory with a view to the commission of a serious crime within its territory;
 - (ii) One of those established in accordance with article 6, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 6, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory.
3. For the purposes of article 16, paragraph 10, of this Convention, each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.
4. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite him or her.
5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.
6. Without prejudice to norms of general international law, this Convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Article 16 - Extradition

1. This article shall apply to the offences covered by this Convention or in cases where an offence referred to in article 3, paragraph 1 (a) or (b), involves an organized criminal group and the person who is the subject of the request for extradition is located in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party.
2. If the request for extradition includes several separate serious crimes, some of which are not covered by this article, the requested State Party may apply this article also in respect of the latter offences.
3. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.
4. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.
5. States Parties that make extradition conditional on the existence of a treaty shall:
 - (a) At the time of deposit of their instrument of ratification, acceptance, approval or accession to this Convention, inform the Secretary-General of the United Nations whether they will take this Convention as the legal basis for cooperation on extradition with other States Parties to this Convention; and
 - (b) If they do not take this Convention as the legal basis for cooperation on extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.
6. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.
7. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.
8. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

9. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent and at the request of the requesting State Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his or her presence at extradition proceedings.

10. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that he or she is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decision and conduct their proceedings in the same manner as in the case of any other offence of a grave nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.

11. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 10 of this article.

12. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting Party, consider the enforcement of the sentence that has been imposed under the domestic law of the requesting Party or the remainder thereof.

13. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present.

14. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, religion, nationality, ethnic origin or political opinions or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

15. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters.

16. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation.

17. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.

Article 17 - Transfer of sentenced persons

States Parties may consider entering into bilateral or multilateral agreements or arrangements on the transfer to their territory of persons sentenced to imprisonment or other forms of deprivation of liberty for offences covered by this Convention, in order that they may complete their sentences there.

13.3.4 2003 UN Convention against Corruption

Article 42 - Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:

- (a) The offence is committed in the territory of that State Party; or
- (b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.

2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

- (a) The offence is committed against a national of that State Party; or
- (b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory; or
- (c) The offence is one of those established in accordance with article 23, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 23, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory; or
- (d) The offence is committed against the State Party.

3. For the purposes of article 44 of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Article 44 - Extradition

1. This article shall apply to the offences established in accordance with this Convention where the person who is the subject of the request for extradition is present in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party.

2. Notwithstanding the provisions of paragraph 1 of this article, a State Party whose law so permits may grant the extradition of a person for any of the offences covered by this Convention that are not punishable under its own domestic law.

3. If the request for extradition includes several separate offences, at least one of which is extraditable under this article and some of which are not extraditable by reason of their period of imprisonment but are related to offences established in accordance with this Convention, the requested State Party may apply this article also in respect of those offences.

4. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them. A State Party whose law so permits, in case it uses this Convention as the basis for extradition, shall not consider any of the offences established in accordance with this Convention to be a political offence.

5. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.

6. A State Party that makes extradition conditional on the existence of a treaty shall:

(a) At the time of deposit of its instrument of ratification, acceptance or approval of or accession to this Convention, inform the Secretary-General of the United Nations whether it will take this Convention as the legal basis for cooperation on extradition with other States Parties to this Convention; and

(b) If it does not take this Convention as the legal basis for cooperation on extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.

7. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.

8. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

9. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

10. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent and at the request of the requesting State Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his or her presence at extradition proceedings.

11. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that he or she is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decision and conduct their proceedings in the same manner as in the case of any other offence of a grave nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.

12. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 11 of this article.

13. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested State Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting State Party, consider the enforcement of the sentence imposed under the domestic law of the requesting State Party or the remainder thereof.

14. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present.

15. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, religion, nationality, ethnic origin or political opinions or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

16. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters.

17. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation.

18. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.

Article 45 - Transfer of sentenced persons

States Parties may consider entering into bilateral or multilateral agreements or arrangements on the transfer to their territory of persons sentenced to imprisonment or other forms of deprivation of liberty for offences established in accordance with this Convention in order that they may complete their sentences there.

13.3.5 Council of the EU Framework Decision on the European arrest warrant and the surrender procedures between Member States

Article 1 – Definition of the European arrest warrant and obligation to execute it

1. The European arrest warrant is a judicial decision issued by a Member State with a view to the arrest and surrender by another Member State of a requested person, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order.

2. Member States shall execute any European arrest warrant on the basis of the principle of mutual recognition and in accordance with the provisions of this Framework Decision.

3. This Framework Decision shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.

Article 2 - Scope of the European arrest warrant

1. A European arrest warrant may be issued for acts punishable by the law of the issuing Member State by a custodial sentence or a detention order for a maximum period of at least 12 months or, where a sentence has been passed or a detention order has been made, for sentences of at least four months.

2. The following offences, if they are punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined by the law of the issuing Member State, shall, under the terms of this Framework Decision and without verification of the double criminality of the act, give rise to surrender pursuant to a European arrest warrant:

- participation in a criminal organisation,- terrorism,
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
- laundering of the proceeds of crime,
- counterfeiting currency, including of the euro,
- computer-related crime,
- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
- facilitation of unauthorised entry and residence,
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and piracy of products,
- forgery of administrative documents and trafficking therein,
- forgery of means of payment,

- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- trafficking in stolen vehicles,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft/ships,
- sabotage.

3. The Council may decide at any time, acting unanimously after consultation of the European Parliament under the conditions laid down in Article 39(1) of the Treaty on European Union (TEU), to add other categories of offence to the list contained in paragraph 2. The Council shall examine, in the light of the report submitted by the Commission pursuant to Article 34(3), whether the list should be extended or amended.

4. For offences other than those covered by paragraph 2, surrender may be subject to the condition that the acts for which the European arrest warrant has been issued constitute an offence under the law of the executing Member State, whatever the constituent elements or however it is described.

13.4 Ratification and implementation

13.4.1 FATF Recommendations

Recommendation 36

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

13.4.2 1998 UN Political Declaration and Action Plan against Money Laundering

The General Assembly

1. Strongly condemns the laundering of money derived from illicit drug trafficking and other serious crimes, as well as the use of the financial systems of States for that purpose;

2. Urges all States to implement the provisions against money-laundering that are contained in the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of 1988 and the other relevant international instruments on money-laundering, in accordance with fundamental constitutional principles, by applying the following principles:

(a) Establishment of a legislative framework to criminalize the laundering of money derived from serious crimes in order to provide for the prevention, detection, investigation and prosecution of the crime of money-laundering through, inter alia:

(i) Identification, freezing, seizure and confiscation of the proceeds of crime;

(ii) International cooperation; and mutual legal assistance in cases involving money-laundering;

(iii) Inclusion of the crime of money-laundering in mutual legal assistance agreements for the purpose of ensuring judicial assistance in investigations, court cases or judicial proceedings relating to that crime;

(b) Establishment of an effective financial and regulatory regime to deny criminals and their illicit funds access to national and international financial systems, thus preserving the integrity of financial systems worldwide and ensuring compliance with laws and other regulations against money-laundering through:

(i) Customer identification and verification requirements applying the principle of "know your customer", in order to have available for competent authorities the necessary information on the identity of clients and the financial movements that they carry out;

(ii) Financial record-keeping;

(iii) Mandatory reporting of suspicious activity;

(iv) Removal of bank secrecy impediments to efforts directed at preventing, investigating and punishing money-laundering;

(v) Other relevant measures;

(c) Implementation of law enforcement measures to provide tools for, inter alia:

(i) Effective detection, investigation, prosecution and conviction of criminals engaging in money-laundering activity;

(ii) Extradition procedures;

(iii) Information-sharing mechanisms;

13.4.3 2001 Conference of the G8 Ministers of Justice and Interior

The Ministers of Justice and Interior of the G 8

12. reaffirm the Principles of the Moscow Communique, which stressed the importance of the fight against money laundering within the strategy of countering transnational organised crime;

13. commend the work of the Financial Action Task Force (FATF) to identify jurisdictions whose anti-money laundering systems do not meet the international standards of the FATF Forty Recommendations, and to take all appropriate measures to bring those non-co-operative jurisdictions into compliance with those standards;

14. strongly reaffirm the need for legislative and administrative measures aimed at assuring transparency of the financial systems. We encourage the development of common principles to remove obstacles, such as bank secrecy, to the rapid and effective implementation of requests for mutual legal assistance in banking and tax matters;

15. will intensify our joint efforts to improve effective international co-operation and mutual legal assistance in the confiscation of illicit assets, including through measures contained in the Palermo Convention and in existing regional and bilateral agreements;

13.4.4 Council of the EU Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime

Article 1 - Reservations in respect of the 1990 Convention

In order to enhance action against organised crime, Member States shall take the necessary steps not to make or uphold reservations in respect of the following articles of the 1990 Convention:

(a) Article 2, in so far as the offence is punishable by deprivation of liberty or a detention order for a maximum of more than one year.

However, Member States may uphold reservations on Article 2 of the 1990 Convention in respect of the confiscation of the proceeds from tax offences for the sole purpose of their being able to confiscate such proceeds, both nationally and through international cooperation, under national, Community and international tax-debt recovery legislation;

(b) Article 6, in so far as serious offences are concerned. Such offences shall in any event include offences which are punishable by deprivation of liberty 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, offences punishable by deprivation of liberty or a detention order for a minimum of more than six months.

13.4.5 2001 Joint ECOFIN/JHA meeting

11. The Council emphasises strongly the importance for all Member States, the Candidate Countries and for dependent and associated territories of Member States to implement fully the Union acquis on the fight against terrorism, money laundering and financial crime, the 40 FATF Recommendations on money laundering and to take appropriate measures to be able to implement the counter-measures recommended by FATF. In particular, the Council welcomes the commitment of the Hungarian Government to improve anti-money laundering standards and urges the speedy adoption by the Hungarian Parliament of the measures required to meet all the FATF recommendations. The Council welcomes the Commission's intention to reinforce the scrutiny of the Candidate Countries' anti-money laundering activities in the Peer Reviews that are now under way.

14 FINANCIAL INTELLIGENCE UNITS (FIU)

14.1.1 FATF 40 Recommendations

Recommendation 29

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

Interpretative note to Recommendation 29

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

4. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination.

- **Spontaneous dissemination:** The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.

9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

12. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

14.1.2 Egmont – Statement of purpose

Definition of Financial Intelligence Unit:

A central, national agency responsible for receiving (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information

(i) concerning suspected proceeds of crime and potential financing of terrorism, or

(ii) required by national legislation or regulation,

in order to combat money laundering and terrorism financing.

14.1.3 Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases

Conditions for the exchange of information

9. FIUs should be able to exchange information freely with other FIUs in the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party. Such exchange, either upon request or spontaneously, should produce any available information that may be relevant to an analysis or investigation of financial transactions and other relevant information related to money laundering and the persons or companies involved.

10. An FIU requesting information should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the receiving FIU to determine whether the request complies with its domestic law.

Permitted uses of information

11. Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.

12. The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information.

Confidentiality – Protection of privacy

13. All information exchanged by FIUs must be subject to strict controls and safeguards to ensure that the information is used only in an authorised manner, consistent with national provisions on privacy and data protection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU.

14.1.4 2003 UN Convention against Corruption

Article 58 - Financial intelligence unit

States Parties shall cooperate with one another for the purpose of preventing and combating the transfer of proceeds of offences established in accordance with this Convention and of promoting ways and means of recovering such proceeds and, to that end, shall consider establishing a financial intelligence unit to be responsible for receiving, analysing and disseminating to the competent authorities reports of suspicious financial transactions.

14.1.5 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 1 – Use of terms

For the purposes of this Convention:

f "financial intelligence unit" (hereinafter referred to as "FIU") means a central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information

- i concerning suspected proceeds and potential financing of terrorism, or
 - ii required by national legislation or regulation,
- in order to combat money laundering and financing of terrorism;

Article 12 – Financial intelligence unit (FIU)

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish an FIU as defined in this Convention.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that its FIU has 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 suspicious transaction reports.

Article 46 – Co-operation between FIUs

- 1 Parties shall ensure that FIUs, as defined in this Convention, shall cooperate for the purpose of combating money laundering, to assemble and analyse, or, if appropriate, investigate within the FIU relevant information on any fact which might be an indication of money laundering in accordance with their national powers.
- 2 For the purposes of paragraph 1, each Party shall ensure that FIUs exchange, spontaneously or on request and either in accordance with this Convention or in accordance with existing or future memoranda of understanding compatible with this Convention, any accessible information that may be relevant to the processing or analysis of information or, if appropriate, to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved.
- 3 Each Party shall ensure that the performance of the functions of the FIUs under this article shall not be affected by their internal status, regardless of whether they are administrative, law enforcement or judicial authorities.
- 4 Each request made under this article shall be accompanied by a brief statement of the relevant facts known to the requesting FIU. The FIU shall specify in the request how the information sought will be used.
- 5 When a request is made in accordance with this article, the requested FIU shall provide all relevant information, including accessible financial information and requested law enforcement data, sought in the request, without the need for a formal letter of request under applicable conventions or agreements between the Parties.
- 6 An FIU may refuse to divulge information which could lead to impairment of a criminal investigation being conducted in the requested Party or, in exceptional circumstances, where divulging the information would be clearly disproportionate to the legitimate interests of a natural or legal person or the Party concerned or would otherwise not be in accordance with fundamental principles of national law of the requested Party. Any such refusal shall be appropriately explained to the FIU requesting the information.
- 7 Information or documents obtained under this article shall only be used for the purposes laid down in paragraph 1. Information supplied by a counterpart FIU shall not be disseminated to a third party, nor be used by the receiving FIU for purposes other than analysis, without prior consent of the supplying FIU.
- 8 When transmitting information or documents pursuant to this article, the transmitting FIU may impose restrictions and conditions on the use of information for purposes other than those stipulated in paragraph 7. The receiving FIU shall comply with any such restrictions and conditions.
- 9 Where a Party wishes to use transmitted information or documents for criminal investigations or prosecutions for the purposes laid down in paragraph 7, the transmitting FIU may not refuse its consent to such use unless it does so on the basis of restrictions under its national law or conditions referred to in paragraph 6. Any refusal to grant consent shall be appropriately explained.
- 10 FIUs shall undertake all necessary measures, including security measures, to ensure that information submitted under this article is not accessible by any other authorities, agencies or departments.

11 The information submitted shall be protected, in conformity with the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and taking account of Recommendation No R(87)15 of 15 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector, by at least the same rules of confidentiality and protection of personal data as those that apply under the national legislation applicable to the requesting FIU.

12 The transmitting FIU may make reasonable enquiries as to the use made of information provided and the receiving FIU shall, whenever practicable, provide such feedback.

13 Parties shall indicate the unit which is an FIU within the meaning of this article.

Article 47 – International co-operation for postponement of suspicious transactions

1 Each Party shall adopt such legislative or other measures as may be necessary to permit urgent action to be initiated by a FIU, at the request of a foreign FIU, to suspend or withhold consent to a transaction going ahead for such periods and depending on the same conditions as apply in its domestic law in respect of the postponement of transactions.

2 The action referred to in paragraph 1 shall be taken where the requested FIU is satisfied, upon justification by the requesting FIU, that:

a the transaction is related to money laundering; and

b the transaction would have been suspended, or consent to the transaction going ahead would have been withheld, if the transaction had been the subject of a domestic suspicious transaction report.

14.1.6 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (as amended)

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 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 38

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

14.1.7 Council of the EU Decision concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information

Article 1

1. Member States shall ensure that FIUs, set up or designated to receive disclosures of financial information for the purpose of combating money laundering shall cooperate to assemble, analyse and investigate relevant information within the FIU on any fact which might be an indication of money laundering in accordance with their national powers.

2. For the purposes of paragraph 1, Member States shall ensure that FIUs exchange, spontaneously or on request and either in accordance with this Decision or in accordance with existing or future memoranda of understanding, any available information that may be relevant to the processing or analysis of information or to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved.

3. Where a Member State has designated a police authority as its FIU, it may supply information held by that FIU to be exchanged pursuant to this Decision to an authority of the receiving Member State designated for that purpose and being competent in the areas mentioned in paragraph 1.

Article 2

1. Member States shall ensure that, for the purposes of this Decision, FIUs shall be a single unit for each Member State and shall correspond to the following definition: "A central, national unit which, in order to combat money laundering,

is responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information which concern suspected proceeds of crime or are required by national legislation or regulation".

2. In the context of paragraph 1, a Member State may establish a central unit for the purpose of receiving or transmitting information to or from decentralised agencies.

3. Member States shall indicate the unit which is an FIU within the meaning of this Article. They shall notify this information to the General Secretariat of the Council in writing. This notification does not affect the current relations concerning cooperation between the FIUs.

Article 3

Member States shall ensure that the performance of the functions of the FIUs under this Decision shall not be affected by their internal status, regardless of whether they are administrative, law enforcement or judicial authorities.

Article 4

1. Each request made under this Decision shall be accompanied by a brief statement of the relevant facts known to the requesting FIU. The FIU shall specify in the request how the information sought will be used.

2. When a request is made in accordance with this Decision, the requested FIU shall provide all relevant information, including available financial information and requested law enforcement data, sought in the request, without the need for a formal letter of request under applicable conventions or agreements between Member States.

3. An FIU may refuse to divulge information which could lead to impairment of a criminal investigation being conducted in the requested Member State or, in exceptional circumstances, where divulgement of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State concerned or would otherwise not be in accordance with fundamental principles of national law. Any such refusal shall be appropriately explained to the FIU requesting the information.

Article 5

1. Information or documents obtained under this Decision are intended to be used for the purposes laid down in Article 1(1).

2. When transmitting information or documents pursuant to this Decision, the transmitting FIU may impose restrictions and conditions on the use of information for purposes other than those stipulated in paragraph 1. The receiving FIU shall comply with any such restrictions and conditions.

3. Where a Member State wishes to use transmitted information or documents for criminal investigations or prosecutions for the purposes laid down in Article 1(1), the transmitting Member State may not refuse its consent to such use unless it does so on the basis of restrictions under its national law or conditions referred to in Article 4(3). Any refusal to grant consent shall be appropriately explained.

4. FIUs shall undertake all necessary measures, including security measures, to ensure that information submitted under this Decision is not accessible by any other authorities, agencies or departments.

5. The information submitted will be protected, in conformity with the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and taking account of Recommendation No R(87)15 of 15 September 1987 of the Council of Europe Regulating the Use of Personal Data in the Police Sector, by at least the same rules of confidentiality and protection of personal data as those that apply under the national legislation applicable to the requesting FIU.

Article 6

1. FIUs may, within the limits of the applicable national law and without a request to that effect, exchange relevant information.

2. Article 5 shall apply in relation to information forwarded under this Article.

Article 7

Member States shall provide for, and agree on, appropriate and protected channels of communication between FIUs.

Article 8

This Decision shall be implemented without prejudice to the Member States' obligations towards Europol, as they have been laid down in the Europol Convention.

Article 9

1. To the extent that the level of cooperation between FIUs, as expressed in memoranda of understanding concluded or to be concluded between authorities of the Member States, is compatible with this Decision or goes further than the provisions thereof, it shall remain unaffected by this Decision. Where the provisions of this Decision go further than the provisions of any memorandum of understanding concluded between the authorities of Member States, this Decision shall supersede such memoranda of understanding two years after this Decision takes effect.

2. The Member States shall ensure that they are able to cooperate fully in accordance with the provisions of this Decision at the latest three years after this Decision takes effect.

3. The Council will assess Member States' compliance with this Decision within four years of the date on which it takes effect, and may decide to continue such assessments on a regular basis.

Article 10

This Decision shall apply to Gibraltar. To this effect, notwithstanding Article 2, the United Kingdom may notify to the General Secretariat of the Council an FIU in Gibraltar.

14.1.8 2001 Joint ECOFIN/JHA meeting

13. The Council reconfirms the importance of close cooperation between Financial Intelligence Units (FIU) of the Member States in respect of exchanging information on suspicious transactions including those related to terrorism. The adoption of the Decision on exchange of information between FIUs at the joint ECOFIN/JHA Council meeting on 17 October 2000 was a significant step in elaborating mutual cooperation between Member States' FIUs. Consequently the Member States have to ensure uniform implementation of the Decision, including providing for appropriate and protected channels of communications between FIUs. The Council confirms the necessity to enhance the communication between FIUs and calls upon the Member States to reinforce the existing system and to examine whether to elaborate a system for exchange of relevant information by automatic means and asks the Commission to explore the possibilities of Community funding for such an automatic system.

15 OTHER ISSUES

15.1 Controlled delivery

15.1.1 FATF Recommendations

Recommendation 30

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

Interpretative note to Recommendation 30

There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation.

2. A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to:
 - identifying the extent of criminal networks and/or the scale of criminality;
 - identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and
 - developing evidence which can be used in criminal proceedings.
3. A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.
4. Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing 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.
5. Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.
6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.
7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.
8. Law enforcement authorities and prosecutorial authorities should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Recommendation 31

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary 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, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence. Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal

persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

15.1.2 1988 UN Convention against illicit traffic in narcotic drugs and psychotropic substances

Article 1

(g) "Controlled delivery" means the technique of allowing illicit or suspect consignments of narcotic drugs, psychotropic substances, substances in Table I and Table II annexed to this Convention, or substances substituted for them, to pass out of, through or into the territory of one or more countries, with the knowledge and under the supervision of their competent authorities, with a view to identifying persons involved in the commission of offences established in accordance with article 3, paragraph 1 of the Convention;

Article 11

1. If permitted by the basic principles of their respective domestic legal systems, the Parties shall take the necessary measures, within their possibilities, to allow for the appropriate use of controlled delivery at the international level, on the basis of agreements or arrangements mutually consented to, with a view to identifying persons involved in offences established in accordance with article 3, paragraph 1, and to taking legal action against them.
2. Decisions to use controlled delivery shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the Parties concerned.
3. Illicit consignments whose controlled delivery is agreed to may, with the consent of the Parties concerned, be intercepted and allowed to continue with the narcotic drugs or psychotropic substances intact or removed or replaced in whole or in part.

15.1.3 2000 UN Convention against Transnational Organized Crime

Article 2 – Use of terms

For the purpose of this Convention.

(i) "Controlled delivery" shall mean the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence;

Article 20 - Special investigative techniques

1. If permitted by the basic principles of its domestic legal system, each State Party shall, within its possibilities and under the conditions prescribed by its domestic law, take the necessary measures to allow for the appropriate use of controlled delivery and, where it deems appropriate, for the use of other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, by its competent authorities in its territory for the purpose of effectively combating organized crime.
2. For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.
3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.
4. Decisions to use controlled delivery at the international level may, with the consent of the States Parties concerned, include methods such as intercepting and allowing the goods to continue intact or be removed or replaced in whole or in part.

15.1.4 2003 UN Convention against Corruption

Article 2- Use of terms

For the purposes of this Convention:

(i) “**Controlled delivery**” shall mean the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence.

Article 50 - Special investigative techniques

1. In order to combat corruption effectively, each State Party shall, to the extent permitted by the basic principles of its domestic legal system and in accordance with the conditions prescribed by its domestic law, take such measures as may be necessary, within its means, to allow for the appropriate use by its competent authorities of controlled delivery and, where it deems appropriate, other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, within its territory, and to allow for the admissibility in court of evidence derived there from.

2. For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.

3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.

4. Decisions to use controlled delivery at the international level may, with the consent of the States Parties concerned, include methods such as intercepting and allowing the goods or funds to continue intact or be removed or replaced in whole or in part.

15.1.5 The 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU

Article 12 - Controlled deliveries

1. Each Member State shall undertake to ensure that, at the request of another Member State, controlled deliveries may be permitted on its territory in the framework of criminal investigations into extraditable offences.

2. The decision to carry out controlled deliveries shall be taken in each individual case by the competent authorities of the requested Member State, with due regard for the national law of that Member State.

3. Controlled deliveries shall take place in accordance with the procedures of the requested Member State. The right to act and to direct and control operations shall lie with the competent authorities of that Member State.

15.2 Cross-border transportation of cash

15.2.1 FATF Recommendations

Definitions

Bearer negotiable instruments Bearer negotiable instruments (BNIs) includes monetary instruments in bearer form such as: traveller’s cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; Incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee’s name omitted.

Currency Currency refers to banknotes and coins that are in circulation as a medium of exchange.

False declaration refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

False disclosure refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

Physical cross-border transportation refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical

transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.

Recommendation 32

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

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, money laundering or predicate offences, 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, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

Interpretative Note to Recommendation 32

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical crossborder transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.

(a) *Written declaration system for all travellers*: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travelers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a "yes" or "no" box).

(b) *Written declaration system for travellers carrying amounts above a threshold*: In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

(c) *Oral declaration system for all travellers*: In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the "red channel" (goods to declare) and the "green channel" (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

5. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

(a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.

(b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs and their intended use.

(c) Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious crossborder transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way.

(d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

(e) In the following two cases, competent authorities should be able to stop or restrain cash or BNIs for a reasonable time, in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

(f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a

declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

(g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.

7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers a unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

15.2.2 2000 UN Convention against Transnational Organized Crime

Article 7 - Measures to combat money-laundering

2. States Parties shall consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders, subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments.

15.2.3 2003 UN Convention against Corruption

Article 14 - Measures to prevent money-laundering

2. States Parties shall consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders, subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments.

15.2.4 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 13 – Measures to prevent money laundering

1 Each Party shall adopt such legislative and other measures as may be necessary to institute a comprehensive domestic regulatory and supervisory or monitoring regime to prevent money laundering and shall take due account of applicable international standards, including in particular the recommendations adopted by the Financial Action Task Force on Money Laundering (FATF).

3 In that respect, each Party shall adopt such legislative or other measures as may be necessary to detect the significant physical cross border transportation of cash and appropriate bearer negotiable instruments.

15.3 Immunity clause

15.3.1 FATF Recommendations

Recommendation 9

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

Recommendation 21

Financial institutions, their directors, officers and employees should be:

- (a) protected by law 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; and
- (b) ...

15.3.2 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist (as amended)

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.

15.4 New techniques

15.4.1 FATF Recommendations

Recommendation 15

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

15.4.2 2000 UN Convention against Transnational Organized Crime

Article 19 - Joint investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigation is to take place is fully respected.

15.4.3 2003 UN Convention against Corruption

Article 14 - Measures to prevent money-laundering

3. States Parties shall consider implementing appropriate and feasible measures to require financial institutions, including money remitters:

- (a) To include on forms for the electronic transfer of funds and related messages accurate and meaningful information on the originator;
- (b) To maintain such information throughout the payment chain; and
- (c) To apply enhanced scrutiny to transfers of funds that do not contain complete information on the originator.

Article 49 - Joint investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigation is to take place is fully respected.

15.4.4 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 7 – Investigative powers and techniques

3 Each Party shall consider adopting such legislative and other measures as may be necessary to enable it to use special investigative techniques facilitating the identification and tracing of proceeds and the gathering of evidence related thereto, such as observation, interception of telecommunications, access to computer systems and order to produce specific documents.

15.5 Targeted financial sanctions related to proliferation

15.5.1 FATF Recommendations

Recommendation 7

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

Interpretative note to Recommendation 7

1. Recommendation 7 requires countries to implement targeted financial sanctions³⁶ to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person³⁷ or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction³⁸.

³⁶ Recommendation 7 is focused on targeted financial sanctions. However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions and vigilance provisions). With respect to other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs. With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction, the FATF has also issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

³⁷ Natural or legal person.

³⁸ Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Recommendation, (February 2012), the Security Council resolutions applying targeted financial

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation³⁹. The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the relevant Security Council Committees. However, in practice, the Committees primarily depend upon requests for designation by Member States. Security Council resolutions 1718 (2006) and 1737(2006) provide that the relevant Committees shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by these resolutions.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

(a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:

(i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions⁴⁰, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

(ii) proposing to the 1737 Sanctions Committee, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 1737 (2006) and its successor resolutions⁴¹, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).

(b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 1737 (2006), and their successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

(c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

(e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the 1737 Sanctions Committee, pursuant to resolution 1737 (2006) and its successor resolutions, providing as much detail as possible on:

(i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

(ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(f) having procedures to be able, where necessary, to operate *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered.

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

(a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council; and

(b) in the case of resolution 1737 (2006) and its successor resolutions, by the Security

sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010).

³⁹ Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and Security Council resolution 1540 (2004). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

⁴⁰ Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009).

⁴¹ Recommendation 7 is applicable to all current and future successor resolutions to S/RES/1737 (2006). At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1737 (2006) are: resolution 1747 (2007), resolution 1803 (2008), and resolution 1929 (2010).

Council in annexes to the relevant resolutions, or by the 1737 Sanctions Committee of the Security Council, when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations.

6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries⁴² should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

(b) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to financial institutions and DNFBBs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBBs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBBs⁴³ to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

(e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 7.

(f) Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBBs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. Such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e., a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

9. Where countries have determined that the exemption conditions set out in resolution 1718 (2006) and resolution 1737 (2006) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 1737 (2006) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

11. Freezing action taken pursuant to resolution 1737 (2006) shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

(a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in the relevant Security Council resolution;

(b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity designated pursuant to resolution 1737 (2006); and

(c) the relevant countries have submitted prior notification to the 1737 Sanctions Committee of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation⁴⁴.

⁴² In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

⁴³ Security Council resolutions apply to all natural and legal persons within the country.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

13. The criteria for designation as specified in the relevant United Nations Security Council resolution are:

(a) **Resolution 1718 (2006):**

- (i) Any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programs;
- (ii) any person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programs, including through illicit means;
- (iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)⁴⁵; or
- (iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)⁴⁶.

(b) **Resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010):**

- (i) any person or entity engaged in Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
- (ii) any person or entity directly associated with or providing support for Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
- (iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i) and/or subsection 13(b)(ii), or by entities owned or controlled by them;
- (iv) any person or entity acting on behalf or at the direction of the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929 (2010);
- (v) any entity owned or controlled, including through illicit means, by the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929 (2010)⁴⁷;
- (vi) any person or entity acting on behalf or at the direction of the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929 (2010);
- (vii) entities owned or controlled, including through illicit means, by the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929 (2010); or
- (viii) any person or entity determined by the United Nations Security Council or the Committee to have assisted designated persons or entities in evading sanction of, or in violating the provisions of, S/RES/1737 (2006), S/RES/1747 (2007), S/RES/1803 (2008), or S/RES/1929 (2010).

⁴⁴ In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, adopted in September 2007.

⁴⁵ The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee.

⁴⁶ Ibid.

⁴⁷ Ibid.

16 TERRORIST FINANCING

16.1.1 FATF Recommendations on Terrorist Financing

Definitions

Appropriate authorities refers to competent authorities, including accrediting institutions, and self-regulatory organisations.

Associate NPOs includes foreign branches of international NPOs.

Designated person or entity refers to:

(i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida;

(ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban;

(iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001);

(iv) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the “Security Council Committee established pursuant to resolution 1718 (2006)” (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and

(v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1737 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the “Security Council Committee established pursuant to paragraph 18 of resolution 1737 (2006)” (the 1737 Sanctions Committee) pursuant to resolution 1737 (2006) and its successor resolutions.

Designation refers to the identification of a person⁴⁸ or entity that is subject to targeted financial sanctions pursuant to:

- United Nations Security Council resolution 1267 (1999) and its successor resolutions;
- Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination;
- Security Council resolution 1718 (2006) and its successor resolutions;
- Security Council resolution 1737 (2006) and its successor resolutions; and
- any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction.

Non-profit organisations refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.

Targeted financial sanctions means both asset freezing and prohibitions

to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

Terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Terrorist act includes: (a) an act which constitutes an offence within the scope of, and as defined in

one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts

against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the

Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).

⁴⁸ Natural or legal.

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.

Terrorist organization refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee or the 1737 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Recommendation 5

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

Interpretative Note to Recommendation 5

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.
2. Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.
3. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with this Recommendation.
4. Terrorist financing offences should extend to any funds, whether from a legitimate or illegitimate source.
5. Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).
6. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.
7. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.
8. Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one forms of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.
9. It should also be an offence to attempt to commit the offence of terrorist financing.
10. It should also be an offence to engage in any of the following types of conduct:
 - (a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;
 - (b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;
 - (c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.
11. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

Recommendation 6

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

Interpretative Note to Recommendation 6

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person⁴⁹ or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions⁵⁰; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)⁵¹. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their own motion, or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions⁵². Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list based programmes, pursuant to those Security Council resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:

- (a) Countries should identify a competent authority or a court as having responsibility for:
 - (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;

⁴⁹ Natural or legal person.

⁵⁰ Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

⁵¹ Based on requirements set, for instance, in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention)* and the *United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention)*, which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the *International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention)* contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

⁵² The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

- (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and
- (iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.
- (b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination whether they are satisfied, according to applicable (supra-) national principles, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2011), as set forth in Section E.
- (c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.
- (d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.
- (e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:
- (i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;
 - (ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;
 - (iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and
 - (iv) specify whether their status as a designating state may be made known.
- (f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:
- (i) follow the procedures for listing, as adopted by the 1988 Committee;
 - (ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and
 - (iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.
- (g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).
- (h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

6. Countries should establish the necessary legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries⁵³ should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(b) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to the financial sector and the DNFBCs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBCs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBCs⁵⁴ to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.

(e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.

8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

9. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are

⁵³ In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

⁵⁴ Security Council resolutions apply to all natural and legal persons within the country.

applied to persons and entities designated by a (supra-)national country pursuant to resolution 1373 (2001) and as set out in resolution 1963 (2010).

11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions**⁵⁵:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof⁵⁶; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.

(b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions**:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.

(c) **Security Council resolution 1373 (2001)**:

(i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;

(ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c)(i) of this subparagraph; or

(iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c)(i) of this subparagraph.

Recommendation 8

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:

(a) by terrorist organisations posing as legitimate entities;

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

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

Interpretative Note to Recommendation 8

1. Non-profit organisations (NPOs) play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The ongoing international campaign against terrorist financing has unfortunately demonstrated, however, that terrorists and terrorist organisations exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. This misuse not only facilitates terrorist activity, but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting the NPO sector from terrorist abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs.

2. NPOs may be vulnerable to abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Depending on the legal form of the NPO and the country, NPOs may often be subject to little or no governmental oversight (for example, registration, record keeping, reporting and monitoring), or few formalities may be required for their creation (for example, there may be no skills or starting capital

⁵⁵ Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012) , the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

⁵⁶ OP2 of resolution 1617 (2005) further defines the criteria for being “associated with” Al-Qaida or Usama bin Laden.

required, no background checks necessary for employees). Terrorist organisations have taken advantage of these characteristics of NPOs to infiltrate the sector and misuse NPO funds and operations to cover for, or support, terrorist activity.

3. The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:

(a) Past and ongoing abuse of the NPO sector by terrorists and terrorist organisations requires countries to adopt measures both: (i) to protect the sector against such abuse, and (ii) to identify and take effective action against those NPOs that either are exploited by, or actively support, terrorists or terrorist organisations.

(b) Measures adopted by countries to protect the NPO sector from terrorist abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote transparency and engender greater confidence in the sector, across the donor community and with the general public, that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of transparency, integrity and public confidence in the management and functioning of all NPOs are integral to ensuring the sector cannot be misused for terrorist financing.

(c) Measures adopted by countries to identify and take effective action against NPOs that either are exploited by, or actively support, terrorists or terrorist organisations should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should, to the extent reasonably possible, avoid any negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

(d) Developing cooperative relationships among the public, private and NPO sector is critical to raising awareness and fostering capabilities to combat terrorist abuse within the sector. Countries should encourage the development of academic research on, and information-sharing in, the NPO sector to address terrorist financing related issues.

(e) A targeted approach in dealing with the terrorist threat to the NPO sector is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.

(f) Flexibility in developing a national response to terrorist financing in the NPO sector is also essential, in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

4. Countries should undertake domestic reviews of their NPO sector, or have the capacity to obtain timely information on its activities, size and other relevant features. In undertaking these assessments, countries should use all available sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are at risk of being misused for terrorist financing.⁵⁷ Countries should also periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

5. There is a diverse range of approaches in identifying, preventing and combating terrorist misuse of NPOs. An effective approach, however, is one that involves all four of the following elements: (a) outreach to the sector, (b) supervision or monitoring, (c) effective investigation and information gathering and (d) effective mechanisms for international cooperation. The following measures represent specific actions that countries should take with respect to each of these elements, in order to protect their NPO sector from terrorist financing abuse.

(a) Outreach to the NPO sector concerning terrorist financing issues

(i) Countries should have clear policies to promote transparency, integrity and public confidence in the administration and management of all NPOs.

(ii) Countries should encourage or undertake outreach programmes to raise awareness in the NPO sector about the vulnerabilities of NPOs to terrorist abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

(iii) Countries should work with the NPO sector to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect the sector from terrorist abuse.

(iv) Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

(b) Supervision or monitoring of the NPO sector Countries should take steps to promote effective supervision or monitoring of their NPO sector. In practice, countries should be able to demonstrate that the following standards apply to NPOs which account for (1) a significant portion of the financial resources under control of the sector; and (2) a substantial share of the sector's international activities.

⁵⁷ For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

- (i) NPOs should maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate authorities.
 - (ii) NPOs should issue annual financial statements that provide detailed breakdowns of incomes and expenditures.
 - (iii) NPOs should be licensed or registered. This information should be available to competent authorities.⁵⁸
 - (iv) NPOs should have appropriate controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities.
 - (v) NPOs should follow a "know your beneficiaries and associate NPOs" rule, which means that the NPO should make best efforts to confirm the identity, credentials and good standing of their beneficiaries and associate NPOs. NPOs should also undertake best efforts to document the identity of their significant donors and to respect donor confidentiality.
 - (vi) NPOs should maintain, for a period of at least five years, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation, and should make these available to competent authorities upon appropriate authority. This also applies to information mentioned in paragraphs (i) and (ii) above.
 - (vii) Appropriate authorities should monitor the compliance of NPOs with the requirements of this Recommendation.⁵⁹ Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.⁶⁰
- (c) Effective information gathering and investigation
- (i) Countries should ensure effective cooperation, coordination and information sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.
 - (ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.
 - (iii) Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.
 - (iv) Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action.
- (d) Effective capacity to respond to international requests for information about an NPO of concern Consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or other forms of terrorist support.
6. Countries should provide their appropriate authorities responsible for supervision, monitoring and investigation of their NPO sector with adequate financial, human and technical resources.

16.1.2 1999 UN International Convention for the Suppression of the Financing of Terrorism

Article 1

For the purposes of this Convention:

1. "**Funds**" means assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.
2. "**State or governmental facility**" means any permanent or temporary facility or conveyance that is used or occupied by representatives of a State, members of Government, the legislature or the judiciary or by officials or employees of a State or any other public authority or entity or by employees or officials of an intergovernmental organization in connection with their official duties.

⁵⁸ Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

⁵⁹ In this context, rules and regulations may include rules and standards applied by self regulatory organisations and accrediting institutions.

⁶⁰ The range of such sanctions might include freezing of accounts, removal of trustees, fines, decertification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

3. "**Proceeds**" means any funds derived from or obtained, directly or indirectly, through the commission of an offence set forth in article 2.

Article 2

1. Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds 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:

(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

2. (a) On depositing its instrument of ratification, acceptance, approval or accession, a State Party which is not a party to a treaty listed in the annex may declare that, in the application of this Convention to the State Party, the treaty shall be deemed not to be included in the annex referred to in paragraph 1, subparagraph (a). The declaration shall cease to have effect as soon as the treaty enters into force for the State Party, which shall notify the depositary of this fact;

(b) When a State Party ceases to be a party to a treaty listed in the annex, it may make a declaration as provided for in this article, with respect to that treaty.

3. For an act to constitute an offence set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offence referred to in paragraph 1, subparagraphs (a) or (b).

4. Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1 of this article.

5. Any person also commits an offence if that person:

(a) Participates as an accomplice in an offence as set forth in paragraph 1 or 4 of this article;

(b) Organizes or directs others to commit an offence as set forth in paragraph 1 or 4 of this article;

(c) Contributes to the commission of one or more offences as set forth in paragraphs 1 or 4 of this article by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either:

(i) Be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of an offence as set forth in paragraph 1 of this article; or

(ii) Be made in the knowledge of the intention of the group to commit an offence as set forth in paragraph 1 of this article.

Article 3

This Convention shall not apply where the offence is committed within a single State, the alleged offender is a national of that State and is present in the territory of that State and no other State has a basis under article 7, paragraph 1, or article 7, paragraph 2, to exercise jurisdiction, except that the provisions of articles 12 to 18 shall, as appropriate, apply in those cases.

Article 4

Each State Party shall adopt such measures as may be necessary:

(a) To establish as criminal offences under its domestic law the offences set forth in article 2;

(b) To make those offences punishable by appropriate penalties which take into account the grave nature of the offences.

Article 5

1. Each State Party, in accordance with its domestic legal principles, shall take the necessary measures to enable a legal entity located in its territory or organized under its laws to be held liable when a person responsible for the management or control of that legal entity has, in that capacity, committed an offence set forth in article 2. Such liability may be criminal, civil or administrative.

2. Such liability is incurred without prejudice to the criminal liability of individuals having committed the offences.

3. Each State Party shall ensure, in particular, that legal entities liable in accordance with paragraph 1 above are subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions. Such sanctions may include monetary sanctions.

Article 6

Each State Party shall adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.

Article 7

1. Each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 when:

(a) The offence is committed in the territory of that State;

- (b) The offence is committed on board a vessel flying the flag of that State or an aircraft registered under the laws of that State at the time the offence is committed;
 - (c) The offence is committed by a national of that State.
2. A State Party may also establish its jurisdiction over any such offence when:
- (a) The offence was directed towards or resulted in the carrying out of an offence referred to in article 2, paragraph 1, subparagraph (a) or (b), in the territory of or against a national of that State;
 - (b) The offence was directed towards or resulted in the carrying out of an offence referred to in article 2, paragraph 1, subparagraph (a) or (b), against a State or government facility of that State abroad, including diplomatic or consular premises of that State;
 - (c) The offence was directed towards or resulted in an offence referred to in article 2, paragraph 1, subparagraph (a) or (b), committed in an attempt to compel that State to do or abstain from doing any act;
 - (d) The offence is committed by a stateless person who has his or her habitual residence in the territory of that State;
 - (e) The offence is committed on board an aircraft which is operated by the Government of that State.
3. Upon ratifying, accepting, approving or acceding to this Convention, each State Party shall notify the Secretary-General of the United Nations of the jurisdiction it has established in accordance with paragraph 2. Should any change take place, the State Party concerned shall immediately notify the Secretary-General.
4. Each State Party shall likewise take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 in cases where the alleged offender is present in its territory and it does not extradite that person to any of the States Parties that have established their jurisdiction in accordance with paragraphs 1 or 2.
5. When more than one State Party claims jurisdiction over the offences set forth in article 2, the relevant States Parties shall strive to coordinate their actions appropriately, in particular concerning the conditions for prosecution and the modalities for mutual legal assistance.
6. Without prejudice to the norms of general international law, this Convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Article 8

1. Each State Party shall take appropriate measures, in accordance with its domestic legal principles, for the identification, detection and freezing or seizure of any funds used or allocated for the purpose of committing the offences set forth in article 2 as well as the proceeds derived from such offences, for purposes of possible forfeiture.
2. Each State Party shall take appropriate measures, in accordance with its domestic legal principles, for the forfeiture of funds used or allocated for the purpose of committing the offences set forth in article 2 and the proceeds derived from such offences.
3. Each State Party concerned may give consideration to concluding agreements on the sharing with other States Parties, on a regular or case-by-case basis, of the funds derived from the forfeitures referred to in this article.
4. Each State Party shall consider establishing mechanisms whereby the funds derived from the forfeitures referred to in this article are utilized to compensate the victims of offences referred to in article 2, paragraph 1, subparagraph (a) or (b), or their families.
5. The provisions of this article shall be implemented without prejudice to the rights of third parties acting in good faith.

Article 9

1. Upon receiving information that a person who has committed or who is alleged to have committed an offence set forth in article 2 may be present in its territory, the State Party concerned shall take such measures as may be necessary under its domestic law to investigate the facts contained in the information.
2. Upon being satisfied that the circumstances so warrant, the State Party in whose territory the offender or alleged offender is present shall take the appropriate measures under its domestic law so as to ensure that person's presence for the purpose of prosecution or extradition.
3. Any person regarding whom the measures referred to in paragraph 2 are being taken shall be entitled to:
 - (a) Communicate without delay with the nearest appropriate representative of the State of which that person is a national or which is otherwise entitled to protect that person's rights or, if that person is a stateless person, the State in the territory of which that person habitually resides;
 - (b) Be visited by a representative of that State;
 - (c) Be informed of that person's rights under subparagraphs (a) and (b).
4. The rights referred to in paragraph 3 shall be exercised in conformity with the laws and regulations of the State in the territory of which the offender or alleged offender is present, subject to the provision that the said laws and regulations must enable full effect to be given to the purposes for which the rights accorded under paragraph 3 are intended.
5. The provisions of paragraphs 3 and 4 shall be without prejudice to the right of any State Party having a claim to jurisdiction in accordance with article 7, paragraph 1, subparagraph (b), or paragraph 2, subparagraph (b), to invite the International Committee of the Red Cross to communicate with and visit the alleged offender.
6. When a State Party, pursuant to the present article, has taken a person into custody, it shall immediately notify, directly or through the Secretary-General of the United Nations, the States Parties which have established jurisdiction in accordance with article 7, paragraph 1 or 2, and, if it considers it advisable, any other interested States Parties, of the fact that such person is in custody and of the circumstances which warrant that person's detention. The State which

makes the investigation contemplated in paragraph 1 shall promptly inform the said States Parties of its findings and shall indicate whether it intends to exercise jurisdiction.

Article 10

1. The State Party in the territory of which the alleged offender is present shall, in cases to which article 7 applies, if it does not extradite that person, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without undue delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State. Those authorities shall take their decision in the same manner as in the case of any other offence of a grave nature under the law of that State.
2. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State to serve the sentence imposed as a result of the trial or proceeding for which the extradition or surrender of the person was sought, and this State and the State seeking the extradition of the person agree with this option and other terms they may deem appropriate, such a conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 1.

Article 11

1. The offences set forth in article 2 shall be deemed to be included as extraditable offences in any extradition treaty existing between any of the States Parties before the entry into force of this Convention. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be subsequently concluded between them.
2. When a State Party which makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, the requested State Party may, at its option, consider this Convention as a legal basis for extradition in respect of the offences set forth in article 2. Extradition shall be subject to the other conditions provided by the law of the requested State.
3. States Parties which do not make extradition conditional on the existence of a treaty shall recognize the offences set forth in article 2 as extraditable offences between themselves, subject to the conditions provided by the law of the requested State.
4. If necessary, the offences set forth in article 2 shall be treated, for the purposes of extradition between States Parties, as if they had been committed not only in the place in which they occurred but also in the territory of the States that have established jurisdiction in accordance with article 7, paragraphs 1 and 2.
5. The provisions of all extradition treaties and arrangements between States Parties with regard to offences set forth in article 2 shall be deemed to be modified as between States Parties to the extent that they are incompatible with this Convention.

Article 12

1. States Parties shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal or extradition proceedings in respect of the offences set forth in article 2, including assistance in obtaining evidence in their possession necessary for the proceedings.
2. States Parties may not refuse a request for mutual legal assistance on the ground of bank secrecy.
3. The requesting Party shall not transmit nor use information or evidence furnished by the requested Party for investigations, prosecutions or proceedings other than those stated in the request without the prior consent of the requested Party.
4. Each State Party may give consideration to establishing mechanisms to share with other States Parties information or evidence needed to establish criminal, civil or administrative liability pursuant to article 5.
5. States Parties shall carry out their obligations under paragraphs 1 and 2 in conformity with any treaties or other arrangements on mutual legal assistance or information exchange that may exist between them. In the absence of such treaties or arrangements, States Parties shall afford one another assistance in accordance with their domestic law.

Article 13

None of the offences set forth in article 2 shall be regarded, for the purposes of extradition or mutual legal assistance, as a fiscal offence. Accordingly, States Parties may not refuse a request for extradition or for mutual legal assistance on the sole ground that it concerns a fiscal offence.

Article 14

None of the offences set forth in article 2 shall be regarded for the purposes of extradition or mutual legal assistance as a political offence or as an offence connected with a political offence or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an offence may not be refused on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives.

Article 15

Nothing in this Convention shall be interpreted as imposing an obligation to extradite or to afford mutual legal assistance, if the requested State Party has substantial grounds for believing that the request for extradition for offences set forth in article 2 or for mutual legal assistance with respect to such offences has been made for the purpose of

prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion or that compliance with the request would cause prejudice to that person's position for any of these reasons.

Article 16

1. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for the investigation or prosecution of offences set forth in article 2 may be transferred if the following conditions are met:

- (a) The person freely gives his or her informed consent;
- (b) The competent authorities of both States agree, subject to such conditions as those States may deem appropriate.

2. For the purposes of the present article:

- (a) The State to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State from which the person was transferred;
- (b) The State to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States;
- (c) The State to which the person is transferred shall not require the State from which the person was transferred to initiate extradition proceedings for the return of the person;
- (d) The person transferred shall receive credit for service of the sentence being served in the State from which he or she was transferred for time spent in the custody of the State to which he or she was transferred.

3. Unless the State Party from which a person is to be transferred in accordance with the present article so agrees, that person, whatever his or her nationality, shall not be prosecuted or detained or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts or convictions anterior to his or her departure from the territory of the State from which such person was transferred.

Article 17

Any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to this Convention shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law.

Article 18

1. States Parties shall cooperate in the prevention of the offences set forth in article 2 by taking all practicable measures, *inter alia*, by adapting their domestic legislation, if necessary, to prevent and counter preparations in their respective territories for the commission of those offences within or outside their territories, including:

- (a) Measures to prohibit in their territories illegal activities of persons and organizations that knowingly encourage, instigate, organize or engage in the commission of offences set forth in article 2;
- (b) Measures requiring financial institutions and other professions involved in financial transactions to utilize the most efficient measures available for the identification of their usual or occasional customers, as well as customers in whose interest accounts are opened, and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity. For this purpose, States Parties shall consider:
 - (i) Adopting regulations prohibiting the opening of accounts the holders or beneficiaries of which are unidentified or unidentifiable, and measures to ensure that such institutions verify the identity of the real owners of such transactions;
 - (ii) With respect to the identification of legal entities, requiring financial institutions, when necessary, to take measures to verify the legal existence and the 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;
 - (iii) Adopting regulations imposing on financial institutions the obligation to report promptly to the competent authorities all complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose, without fear of assuming criminal or civil liability for breach of any restriction on disclosure of information if they report their suspicions in good faith;
 - (iv) Requiring financial institutions to maintain, for at least five years, all necessary records on transactions, both domestic or international.

2. States Parties shall further cooperate in the prevention of offences set forth in article 2 by considering:

- (a) Measures for the supervision, including, for example, the licensing, of all money transmission agencies;
- (b) Feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

3. States Parties shall further cooperate in the prevention of the offences set forth in article 2 by exchanging accurate and verified information in accordance with their domestic law and coordinating administrative and other measures taken, as appropriate, to prevent the commission of offences set forth in article 2, in particular by:

- (a) Establishing and maintaining channels of communication between their competent agencies and services to facilitate the secure and rapid exchange of information concerning all aspects of offences set forth in article 2;

- (b) Cooperating with one another in conducting inquiries, with respect to the offences set forth in article 2, concerning:
 - (i) The identity, whereabouts and activities of persons in respect of whom reasonable suspicion exists that they are involved in such offences;
 - (ii) The movement of funds relating to the commission of such offences.
4. States Parties may exchange information through the International Criminal Police Organization (Interpol).

16.1.3 UN Resolution 1373

1. Decides that all States shall:

- (a) Prevent and suppress the financing of terrorist acts;
- (b) Criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;
- (c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;
- (d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons;

2. Decides also that all States shall:

- (a) Refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists;
- (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;
- (c) Deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens;
- (d) Prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens;
- (e) Ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts;
- (f) Afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings;
- (g) Prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents;

3. Calls upon all States to:

- (a) Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups;
- (b) Exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts;
- (c) Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts;
- (d) Become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;
- (e) Increase cooperation and fully implement the relevant international conventions and protocols relating to terrorism and Security Council resolutions 1269 (1999) and 1368 (2001);
- (f) Take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum-seeker has not planned, facilitated or participated in the commission of terrorist acts;
- (g) Ensure, in conformity with international law, that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts, and that claims of political motivation are not recognized as grounds for refusing requests for the extradition of alleged terrorists;

4. Notes with concern the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and in this regard emphasizes the need to enhance coordination of efforts on national, subregional, regional and international levels in order to strengthen a global response to this serious challenge and threat to international security;

16.1.4 2005 Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism

Article 1 – Use of terms

For the purposes of this Convention:

h "financing of terrorism" means the acts set out in Article 2 of the International Convention for the Suppression of the Financing of Terrorism, cited above.

Article 2 – Application of the Convention to the financing of terrorism

1 Each Party shall adopt such legislative and other measures as may be necessary to enable it to apply the provisions contained in Chapters III, IV and V of this Convention to the financing of terrorism.

2 In particular, each Party shall ensure that it is able to search, trace, identify, freeze, seize and confiscate property, of a licit or illicit origin, used or allocated to be used by any means, in whole or in part, for the financing of terrorism, or the proceeds of this offence, and to provide co-operation to this end to the widest possible extent.

16.1.5 Wolfsberg Statement on the suppression of the financing of terrorism

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.
- 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.

16.1.6 Council of the EU Framework Decision on combating terrorism

Article 1 Terrorist offences and fundamental rights and principles

1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:

- seriously intimidating a population, or
- unduly compelling a Government or international organisation to perform or abstain from performing any act, or
- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation,

shall be deemed to be terrorist offences:

- (a) attacks upon a person's life which may cause death;
- (b) attacks upon the physical integrity of a person;
- (c) kidnapping or hostage taking;

- (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
 - (e) seizure of aircraft, ships or other means of public or goods transport;
 - (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
 - (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
 - (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
 - (i) threatening to commit any of the acts listed in (a) to (h).
2. This Framework Decision shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.

Article 2 Offences relating to a terrorist group

1. For the purposes of this Framework Decision, "terrorist group" shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.
2. Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:
- (a) directing a terrorist group;
 - (b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Article 3 Offences linked to terrorist activities

- Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts:
- (a) aggravated theft with a view to committing one of the acts listed in Article 1(1);
 - (b) extortion with a view to the perpetration of one of the acts listed in Article 1(1);
 - (c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

Article 4 Inciting, aiding or abetting, and attempting

1. Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.
2. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3, with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable.

Article 5 Penalties

1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 1 to 4 are punishable by effective, proportionate and dissuasive criminal penalties, which may entail extradition.
2. Each Member State shall take the necessary measures to ensure that the terrorist offences referred to in Article 1(1) and offences referred to in Article 4, inasmuch as they relate to terrorist offences, are punishable by custodial sentences heavier than those imposable under national law for such offences in the absence of the special intent required pursuant to Article 1(1), save where the sentences imposable are already the maximum possible sentences under national law.
3. Each Member State shall take the necessary measures to ensure that offences listed in Article 2 are punishable by custodial sentences, with a maximum sentence of not less than fifteen years for the offence referred to in Article 2(2)(a), and for the offences listed in Article 2(2)(b) a maximum sentence of not less than eight years. In so far as the offence referred to in Article 2(2)(a) refers only to the act in Article 1(1)(i), the maximum sentence shall not be less than eight years.

Article 6 Particular circumstances

- Each Member State may take the necessary measures to ensure that the penalties referred to in Article 5 may be reduced if the offender:
- (a) renounces terrorist activity, and
 - (b) provides the administrative or judicial authorities with information which they would not otherwise have been able to obtain, helping them to:
 - (i) prevent or mitigate the effects of the offence;
 - (ii) identify or bring to justice the other offenders;
 - (iii) find evidence; or
 - (iv) prevent further offences referred to in Articles 1 to 4.

Article 7 Liability of legal persons

1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for any of the offences referred to in Articles 1 to 4 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 one of the following:

- (a) a power of representation of the legal person;
- (b) an authority to take decisions on behalf of the legal person;
- (c) an authority to exercise control within the legal person.

2. Apart from the cases provided for in paragraph 1, each Member State shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of any of the offences referred to in Articles 1 to 4 for the benefit of that legal person by a person under its authority.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories in any of the offences referred to in Articles 1 to 4.

Article 8 Penalties for legal persons

Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 7 is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other penalties, such as:

- (a) exclusion from entitlement to public benefits or aid;
- (b) temporary or permanent disqualification from the practice of commercial activities;
- (c) placing under judicial supervision;
- (d) a judicial winding-up order;
- (e) temporary or permanent closure of establishments which have been used for committing the offence.

Article 9 Jurisdiction and prosecution

1. Each Member State shall take the necessary measures to establish its jurisdiction over the offences referred to in Articles 1 to 4 where:

- (a) the offence is committed in whole or in part in its territory. Each Member State may extend its jurisdiction if the offence is committed in the territory of a Member State;
- (b) the offence is committed on board a vessel flying its flag or an aircraft registered there;
- (c) the offender is one of its nationals or residents;
- (d) the offence is committed for the benefit of a legal person established in its territory;
- (e) the offence is committed against the institutions or people of the Member State in question or against an institution of the European Union or a body set up in accordance with the Treaty establishing the European Community or the Treaty on European Union and based in that Member State.

2. When an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account shall be taken of the following factors:

- the Member State shall be that in the territory of which the acts were committed,
- the Member State shall be that of which the perpetrator is a national or resident,
- the Member State shall be the Member State of origin of the victims,
- the Member State shall be that in the territory of which the perpetrator was found.

3. Each Member State shall take the necessary measures also to establish its jurisdiction over the offences referred to in Articles 1 to 4 in cases where it refuses to hand over or extradite a person suspected or convicted of such an offence to another Member State or to a third country.

4. Each Member State shall ensure that its jurisdiction covers cases in which any of the offences referred to in Articles 2 and 4 has been committed in whole or in part within its territory, wherever the terrorist group is based or pursues its criminal activities.

5. This Article shall not exclude the exercise of jurisdiction in criminal matters as laid down by a Member State in accordance with its national legislation.