Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

Annexes

2002-2003

ANNEXES

ANNEX A

THE FATF FORTY RECOMMENDATIONS

Introduction

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

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

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

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

In October 2001 the FATF expanded its mandate to deal with the issue of the financing of terrorism, and took the important step of creating the Eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organisations, and are complementary to the Forty Recommendations[2].

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

---

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

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

THE FORTY RECOMMENDATIONS

A. LEGAL SYSTEMS

Scope of the Criminal Offence of Money Laundering

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

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

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

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

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

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

2. Countries should ensure that:

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

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

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

Provisonal Measures and Confiscation

3. Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

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

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

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

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

Customer Due Diligence and Record-keeping

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

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

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

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

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

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

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

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

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

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

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

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

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

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
b) Obtain senior management approval for establishing business relationships with such customers.
c) Take reasonable measures to establish the source of wealth and source of funds.
d) Conduct enhanced ongoing monitoring of the business relationship.

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

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

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

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.
b) Assess the respondent institution's anti-money laundering and terrorist financing controls.
c) Obtain approval from senior management before establishing new correspondent relationships.
d) Document the respective responsibilities of each institution.
e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

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

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

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

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

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

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

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

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

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

12.* The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

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

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

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

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

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

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

Reporting of Suspicious Transactions and Compliance

13.* If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

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

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

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

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

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
b) An ongoing employee training programme.
c) An audit function to test the system.

16.* The requirements set out in Recommendations 13 to 15, and 21 apply to all designated 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 Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

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

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

Other Measures to Deter Money Laundering and Terrorist Financing

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

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

19.* Countries should consider:

a) Implementing feasible measures to detect or monitor the physical cross-border transportation of currency 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.

b) The feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to

competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

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

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

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

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

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

Regulation and Supervision

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

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

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

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

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

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

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

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

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

Competent Authorities, their Powers and Resources

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

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

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

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

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

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

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

Transparency of legal persons and arrangements

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

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

D. INTERNATIONAL CO-OPERATION

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

Mutual legal assistance and extradition

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

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

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

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

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

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

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

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

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

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

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

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

Other forms of Co-operation

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

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

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

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

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

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

GLOSSARY

In these Recommendations the following abbreviations and references are used:

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

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

"**Designated categories of offences**" means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

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

"**Designated non-financial businesses and professions**" means**:**

a) Casinos (which also includes internet casinos).
b) Real estate agents.
c) Dealers in precious metals.
d) Dealers in precious stones.
e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

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

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

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

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

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   (a) money market instruments (cheques, bills, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance[9].
13. Money and currency changing.

[5] This also captures private banking.

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

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

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

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

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

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

"**FIU**" means Financial Intelligence Unit.

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

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

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

"**Politically Exposed Persons**" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

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

"STR" refers to suspicious transaction reports.

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

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

ANNEX

INTERPRETATIVE NOTES TO THE FORTY RECOMMENDATIONS

INTERPRETATIVE NOTES

General

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

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

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

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

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

Recommendations 5, 12 and 16

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

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

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

Recommendation 5

Customer Due Diligence and tipping off

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

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

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

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

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

CDD for legal persons and arrangements

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

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

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

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

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

Reliance on identification and verification already performed

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

Timing of verification

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

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

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

Requirement to identify existing customers

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

Simplified or reduced CDD measures

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

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

- Financial institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.
- Public companies that are subject to regulatory disclosure requirements.
- Government administrations or enterprises.

[10] "Basel CDD paper" refers to the guidance paper on Customer Due Diligence for Banks issued by the Basel Committee on Banking Supervision in October 2001.

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

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

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

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

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

Recommendation 6

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

Recommendation 9

This Recommendation does not apply to outsourcing or agency relationships.

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

Recommendations 10 and 11

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

Recommendation 13

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

   a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or
   b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

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

2. In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.

Recommendation 14 (tipping off)

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

Recommendation 15

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

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

Recommendation 16

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

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

Recommendation 19

1. To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, countries could consider the feasibility of subjecting all cross-border transfers, above a given threshold, to verification, administrative monitoring, declaration or record keeping requirements.

2. If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

Recommendation 23

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or "fit and proper") tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 25

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

Recommendation 26

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

Recommendation 27

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

Recommendation 38

Countries should consider:

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

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

Recommendation 40

1. For the purposes of this Recommendation:

- "Counterparts" refers to authorities that exercise similar responsibilities and functions.

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

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

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

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

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

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

ANNEX B

Guidance on Implementing the Eight Special Recommendations

Interpretative Note to Special Recommendation VI: Alternative Remittance

General

1. Money or value transfer systems have shown themselves vulnerable to misuse for money laundering and terrorist financing purposes. The objective of Special Recommendation VI is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not currently subject to the FATF Recommendations. This Recommendation and Interpretative Note underscore the need to bring all money or value transfer services, whether formal or informal, within the ambit of certain minimum legal and regulatory requirements in accordance with the relevant FATF Recommendations.

2. Special Recommendation VI consists of three core elements:

a. Jurisdictions should require licensing or registration of persons (natural or legal) that provide money/value transfer services, including through informal systems;

b. Jurisdictions should ensure that money/value transmission services, including informal systems (as described in paragraph 5 below), are subject to applicable FATF Forty Recommendations (in particular, Recommendations 10-21 and 26-29) and the Eight Special Recommendations (in particular SR VII); and

c. Jurisdictions should be able to impose sanctions on money/value transfer services, including informal systems, that operate without a license or registration and that fail to comply with relevant FATF Recommendations.

Scope and Application

3. For the purposes of this Recommendation, the following definitions are used.

4. *Money or value transfer service* refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.

5. A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground (*or *parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala, hundi, fei-chien,* and the *black market peso exchange*.[1]

[1] The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.

6. *Licensing* means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally.

7. *Registration* in this Recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.

8. The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents which must be made available to the designated competent authority. An *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).

Applicability of Special Recommendation VI

9. Special Recommendation VI should apply to all persons (natural or legal), which conduct for or on behalf of another person (natural or legal) the types of activity described in paragraphs 4 and 5 above as a primary or substantial part of their business or when such activity is undertaken on a regular or recurring basis, including as an ancillary part of a separate business enterprise.

10. Jurisdictions need not impose a separate licensing / registration system or designate another competent authority in respect to persons (natural or legal) already licensed or registered as financial institutions (as defined by the FATF Forty Recommendations) within a particular jurisdiction, which under such license or registration are permitted to perform activities indicated in paragraphs 4 and 5 above and which are already subject to the full range of applicable obligations under the FATF Forty Recommendations (in particular, Recommendations 10-21 and 26-29) and the Eight Special Recommendations (in particular SR VII).

Licensing or Registration and Compliance

11. Jurisdictions should designate an authority to grant licences and/or carry out registration and ensure that the requirement is observed. There should be an authority responsible for ensuring compliance by money/value transfer services with the FATF Recommendations (including the Eight Special Recommendations). There should also be effective systems in place for monitoring and ensuring such compliance. This interpretation of Special Recommendation VI (i.e., the need for designation of competent authorities) is consistent with FATF Recommendation 26.

Sanctions

12. Persons providing money/value transfer services without a license or registration should be subject to appropriate administrative, civil or criminal sanctions.[2] Licensed or registered money/value transfer services which fail to comply fully with the relevant measures called for in the FATF Forty Recommendations or the Eight Special Recommendations should also be subject to appropriate sanctions.

[2] Jurisdictions may authorise temporary or provisional operation of money / value transfer services that are already in existence at the time of implementing this Special Recommendation to permit such services to obtain a license or to register.

Interpretative Note to Special Recommendation VII: Wire Transfers[3]

Objective

1. Special Recommendation VII (SR VII) 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 of wire transfers is immediately available (1) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (2) to financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary, and (3) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions. 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.

Definitions

2. For the purposes of this interpretative note, the following definitions apply.

a. The terms *wire transfer* and *funds transfer* refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

b. *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.

c. *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction.

d. The term *financial institution* is as defined by the FATF Forty Recommendations. The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds[4].

e. The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

Scope

3. SR VII applies, under the conditions set out below, to cross-border and domestic transfers between financial institutions.

[3] It is recognised that jurisdictions will need time to make relevant legislative or regulatory changes and to allow financial institutions to make necessary adaptations to their systems and procedures. This period should not be longer than two years after the adoption of this Interpretative Note.

[4] However, these systems do have a role in providing the necessary means for the financial institutions to fulfil their obligations under SR VII and, in particular, in preserving the integrity of the information transmitted with a wire transfer.

Cross-border wire transfers

4. Cross-border wire transfers should be accompanied by accurate and meaningful originator information.[5]

5. Information accompanying cross-border wire transfers must always contain the name of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included.

6. Information accompanying the wire transfer should also contain the address of the originator. However, jurisdictions may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth.

7. Cross-border wire transfers that are contained within batch transfers, except for those sent by money remitters, will be treated as domestic wire transfers. In such cases, the ordering institutions must retain the information necessary to identify all originators and make it available on request to the authorities and to the beneficiary financial institution. Financial institutions should ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

Domestic wire transfers

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

9. The information must 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 authorities. Law enforcement authorities should be able to compel immediate production of such information.

Exemptions from SR VII

10. SR VII 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 card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, 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] Jurisdictions may have a *de minimis* threshold (no higher than USD 3,000) for a one-year period from publication of this Interpretative Note. At the end of this period, the FATF will undertake a review of this issue to determine whether the use of a *de minimis* threshold is acceptable. Notwithstanding any thresholds, accurate and meaningful originator information must be retained and made available by the ordering financing institution as set forth in paragraph 9.

Role of ordering, intermediary and beneficiary financial institutions

Ordering financial institution

11. The ordering financial institution must ensure that qualifying wire transfers contain complete originator information. The ordering financial institution must also verify this information for accuracy and maintain this information in accordance with the standards set out in the FATF Forty Recommendations.

Intermediary financial institution

12. For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

13. Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

Beneficiary financial institution

14. Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet SRVII standards.

Enforcement mechanisms for financial institutions that do not comply with wire transfer rules and regulations

15. Jurisdictions should adopt appropriate measures to monitor effectively the compliance of financial institutions with rules and regulations governing wire transfers. Financial institutions that fail to comply with such rules and regulations should be subject to civil, administrative or criminal sanctions.

Combating The Abuse Of Alternative Remittance Systems

International Best Practices[6]

Introduction

1. Alternative remittance systems are financial services, traditionally operating outside the conventional financial sector, where value or funds are moved from one geographic location to another.

Special Recommendation VI: Alternative Remittance[7]

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

2. While the Interpretative Note is intended to further explain Special Recommendation VI, the Best Practices Paper is intended to give additional details (including some examples), to offer jurisdictions suggestions in implementing Special Recommendation VI and to give them guidance on how to detect alternative remittance systems outside the conventional financial sector. It focuses on many practical issues, such as the identification of money/value transfer services, the procedures for licensing or registering such services and their customer due diligence procedures. This Best Practices Paper addresses the following topics:

- Definition of *money or value transfer service*
- Statement of Problem
- Principles
- Areas of Focus
  - (i) Licensing/Registration
    - a. Requirement to Register or License
    - b. Applications for Licence
    - c. Business Address
    - d. Accounts
  - (ii) Identification and Awareness Raising
    - a. Identification Strategies
    - b. Awareness Raising Campaigns
  - (iii) Anti-Money Laundering Regulations
    - a. Customer Identification
    - b. Record Keeping Requirement
    - c. Suspicious Transaction Reporting
  - (iv) Compliance Monitoring
  - (v) Sanctions

[6] The content of this paper is taken primarily from APG's Draft Alternative Remittance Regulation Implementation Package (Oct 2002.) This Best Practices Paper is intended to draw on the work of the APG Working Group on Underground Banking and Alternative Remittance Systems guided by Mark Butler and Rachelle Boyle, into international best practices.

[7] See also the FATF Interpretative Note to Special Recommendation VI: Alternative Remittance.

Definition

3. Throughout this Best Practices Paper, the following definition from the Interpretative Note to SR VI is used.

4. *Money or value transfer service* (MVT service) refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the MVT service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.

5. A MVT service may be provided by persons (natural or legal) formally through the regulated financial system or informally through entities that operate outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground* (or *parallel*) *banking systems.* Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala, hundi, fei-chien,* and the *black market peso exchange.*

Statement of Problem

6. As 'Know Your Customer' and other anti-money laundering strategies come into operation in the formal financial sector, money laundering activity may be displaced to other sectors. Jurisdictions have reported increased money laundering activity using the non-bank sector and non-financial businesses. Measures should therefore be taken to obviate any increased abuse of the unregulated sector. MVT services are increasingly vulnerable to abuse by money launderers and the financiers of terrorism, particularly when their operations are conducted through informal systems involving non-bank financial institutions or other business entities not subject to the applicable obligations under the FATF Recommendations.

7. In addition to their use by legitimate clients, criminals have laundered the proceeds of various criminal activities using MVT services. Primarily, unregulated MVT services permit funds to be sent anonymously, allowing the money launderer or terrorist financier to freely send funds without having to identify himself or herself. In some cases, few or no records are kept. In other cases, records may be kept, but are inaccessible to authorities. The lack of adequate records makes it extremely difficult, if not impossible, to trace the funds after the transaction has been completed.

8. From recent research, it is suspected that the principal criminal activities engaged in by those who utilise MVT services are the illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking, corruption, evasion of government taxes and duties, trafficking in human beings and migrant smuggling. Recent reports indicate that international terrorist groups have used MVT services to transmit funds for the purpose of funding terrorist activities. (For example, investigation of the September 11, 2001 terrorist attacks has found that both the formal financial sector and informal MVT services were used to transfer money to the terrorists.)

Principles

9. The following principles guide the establishment of these best practices:

- In certain jurisdictions, informal MVT services provide a legitimate and efficient service. Their services are particularly relevant where access to the formal financial sector is difficult or prohibitively expensive. Informal MVT services are available outside the normal banking business hours. Furthermore, money can be sent to and from locations where the formal banking system does not operate.

- Informal MVT services are more entrenched in some regions than others for cultural and other reasons. Underground banking is a long-standing tradition in many countries and pre-dates the spread of Western banking systems in the 19th and 20th centuries. These services operate primarily to provide transfer facilities to neighbouring jurisdictions for expatriate workers repatriating funds. However, the staging posts of underground banking are no longer confined to those regions where they have their historical roots. Accordingly, informal MVT services are no longer used solely by persons from specific ethnic or cultural backgrounds.

- MVT services can take on a variety of forms which, in addition to the adoption of a risk-based approach to the problem, points to the need to take a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to reduce the likelihood that MVT services will be misused or exploited by money launderers and the financiers of terrorism.

- Government oversight should be flexible, effective, and proportional to the risk of abuse. Mechanisms that minimise the compliance burden, without creating loopholes for money launderers and terrorist financiers and without being so burdensome that it in effect causes MVT services to go "underground" making them even harder to detect should be given due consideration.

- It is acknowledged that in some jurisdictions informal MVT services have been banned. Special Recommendation VI does not seek legitimisation of informal MVT services in those jurisdictions. The identification and awareness raising issues noted may however be of use for competent authorities involved in identifying informal MVT services and for sanctioning those who operate illegally.

Areas of Focus

10. Analysis of the investigations and law-enforcement activities of various jurisdictions indicate several ways in which informal MVT services have been abused by terrorists and launderers and suggests areas in which preventive measures should be considered.

(i) Licensing/Registration

11. A core element of Special Recommendation VI is that jurisdictions should require licensing or registration of persons (natural or legal) that provide informal MVT services. The FATF defines these terms in its interpretative note to Special Recommendation VI. A key element of both registration and licensing is the requirement that the relevant regulatory body is aware of the existence of the business. The key difference between the two is that licensing implies that the regulatory body has inspected and sanctioned the particular operator to conduct such a business whereas registration means that the operator has been entered into the regulator's list of operators.

a. Requirement to Register or License

- At a minimum, jurisdictions should ensure that MVT services are required to register with a designated competent authority such as a Financial Intelligence Unit (FIU) or financial sector regulatory body. Registration of MVT services is likely to be a relatively cost effective approach when compared to the significant resources required for licensing.

- The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents which must be made available to the designated competent authority. An agent is any person who provides MVT service under the direction of or by contract with a legally registered or licensed MVT service (for example, licensees, franchisees, concessionaires.

b. Applications for Licence

- In determining whether an application for licensing can be accepted by the regulatory authority, it is clear that some form of scrutiny of the application and the operator needs to be conducted. This is in line with FATF Recommendation 23[8] which states that regulators should introduce "*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.*"

- Authorities should conduct background checks on the operators, owners, directors and shareholders of MVT services. When considering the suitability of a potential operator, the authorities should conduct a criminal record check on the principal persons having control over the operations of the MVT service, as well as consult appropriate law enforcement databases, including suspicious or unusual reporting filings. Consideration should be given to defining the type of criminal record which would make the applicant ineligible to operate a licensed MVT service.

c. Business Address

- MVT services should be required to submit details of the addresses from which they operate and to notify the authorities upon any change of address or cessation of business. Where possible, this information may be made available to both the public so they may check which MVT service is properly licensed or registered before using their services, and to investigative / regulatory authorities during the course of their work. This also has value for financial institutions with which the MVT services maintain accounts as they are able to identify which MVT services are licensed / registered and thus are more able to identify illegal operators and to report to the FIU or appropriate competent authority accordingly.

d. Accounts

- In processing cash and in the settlement of transactions, MVT services use bank accounts. Some operators run a number of businesses, of which MVT service is one, and use business accounts to conduct or conceal the remittances of funds on behalf of their clients thereby masking the true origin of the commingled funds and accounts.

- MVT services should maintain the name and address of any depository institution with which the operator maintains a transaction account for the purpose of the MVT service business. These accounts must be capable of being identified and should be held in the name of the registered/licensed entity so that the accounts and the register or list of licensed entities can be easily cross-referenced.

- Traditional financial institutions should be encouraged to develop more detailed understanding as to how MVT services utilise bank accounts to conduct their operations, particularly when accounts are used in the settlement process.

[8] When this Best Practices Paper was originally issued, these references were to the 1996 FATF Forty Recommendations. Subsequent to the publication of the revised FATF Forty Recommendations in June 2003, this text was updated accordingly. All references are now to the 2003 FATF Forty Recommendations.

(ii) Identification and Awareness Raising

12. Some informal MVT services are not known to regulatory and enforcement agencies, which makes them attractive to the financiers of terrorism. Identification of these MVT services will make it less attractive for criminal and terrorist groups to use them to facilitate and hide the financing of their activities.

13. For the majority of jurisdictions, proactive identification of informal MVT services is an integral element of establishing and maintaining an effective registration / licensing regime. Once informal MVT services have been located, compliance programs can be instituted under which the agents are approached, their details are recorded and they are provided information as to their obligations. Once regulatory regimes are in place, ongoing compliance work will include strategies to identify those MVT services not yet known to regulatory authorities. Jurisdictions may apply a range of strategies to uncover MVT services, using a number of approaches concurrently. Jurisdictions are encouraged to foster close co-ordination within the relevant authorities for the purposes of developing inter-agency strategies and using available resources to identify MVT services that may be operating illegally. Below is a list of suggested best practices for identifying MVT services and raising public awareness about their activities. As best practices, it is recognized that some of these suggestions may not be appropriate for every jurisdiction and that each jurisdiction must develop strategies best suited to its individual system.

a. Identification Strategies

14. Best practices in the area of identification strategies include:

- Examining the full range of media to detect advertising conducted by informal MVT services and informing operators of their registration/licensing obligations. This includes national, local and community newspapers, radio and the Internet; giving particular attention to the printed media in various communities; and monitoring activities in certain neighbourhoods or areas where informal MVT services may be operating.

- During investigations, information about informal MVT services may be uncovered which should be passed on to the competent authorities. Best practices include encouraging investigators to pay particular attention to ledgers of business that may be associated with informal MVT services; encouraging enforcement agencies to look for patterns of activity that might indicate involvement of informal MVT services; and, where possible, encouraging enforcement agencies to consider using undercover techniques or other specific investigative techniques to detect MVT services that may be operating illegally.

- Consulting with the operators of registered / licensed MVT services for potential leads on MVT services that are unregistered or unlicensed.

- Being aware that informal MVT services are often utilised where there is bulk currency moved internationally, particularly when couriers are involved. Paying particular attention to the origin and owners of any such currency. Couriers could provide insights for the identification and potential prosecution of illegal operators with whom the couriers are associated, especially when potential violations by couriers are linked back to the source of the informal MVT service operation.

- Paying particular attention to domestic suspicious transaction or unusual activity reporting, as well as to domestic and international large value cash reporting, to identify possible links to informal MVT services.

- Assisting banks and other financial institutions in developing an understanding of what activities/indicators are suggestive of informal MVT service operations and using this to identify them. Many informal MVT services maintain bank accounts and conduct transactions in the formal financial sector as part of other business operations. Giving banks the authority to cross-check particular accounts against a register of these operators and notify the relevant regulatory authority as appropriate.
- Once informal MVT services are identified international exchange of information and intelligence on these entities between the relevant bodies can be facilitated. Consideration could be given to sharing domestic registers with international counterparts. This strategy would also assist jurisdictions to identify local operators not previously known.

b. Awareness Raising Campaigns

15. Best practices in the area of awareness raising campaigns include:

- Making informal MVT services aware of their obligations to license or register, as well as any other obligations with which they may have to comply. Ensuring that the competent authorities responsible for overseeing and/or registering or licensing informal MVT services know how to detect those services that have not registered or been licensed. Finally, ensuring that law enforcement is aware of the compliance requirements for MVT services in addition to the methods by which those services are used for illicit purposes.

- Using education and compliance programs, including visits to businesses which may be operating informal MVT services to advise them of licensing or registration and reporting obligations, as opportunities to seek information about others in their industry. Using these outreach efforts by law enforcement and regulatory agencies to enhance their understanding about the operations, record-keeping functions and customer bases of informal MVT services. Extending outreach campaigns to businesses typically servicing informal MVT services (such as shipping services, courier services and trading companies). Placing in trade journals, newspapers or other publications of general distribution notices of the need for informal MVT services to register or license and file reports.

- Ensuring that the full range of training, awareness opportunities and other forms of education are provided to investigators with information about MVT services, their obligations under the regulatory regime and ways in which their services can be used by money launderers and terrorist financiers. This information can be provided through training courses, presentations at seminars and conferences, articles in policing journals and other publications.

- Issuing various financial sector publications of guidelines to encourage licensing or registration and reporting and also general material to ensure financial institutions currently subject to suspicious transaction reporting requirements develop an understanding of MVT services. (Also see section on suspicious transaction reporting on page 9.) Informing potential customers about the risks of utilising illegal MVT services and their role in financing of terrorism and money laundering.

- Requiring entities to display their registration/license to customers once they are registered/licensed. Legitimate clients will likely have a higher degree of confidence in using registered/licensed operators and may therefore seek out those operators displaying such documentation.

- Making a list of all licensed or registered persons that provide MVT services publicly available.

(iii) Anti-Money Laundering Regulations

16. The second element of Special Recommendation VI is that jurisdictions should ensure MVT services are subject to FATF Recommendations 4-16 and 21-25 and also to the Eight Special Recommendations.

17. There is key information that both regulatory and enforcement bodies need access to if they are to conduct effective investigations of money laundering and terrorist financing involving MVT services. Essentially, agencies need the information about the customers, the transactions themselves, any suspicious transactions, the MVT service's location and the accounts used. The MVT service must also have further records on hand available to regulatory and enforcement bodies as needed.

18. It is considered that to be effective in addressing the problem of MVT services, regulations should not be overly restrictive. Regulation must allow for those who abuse these systems to be found and stopped, but it should not be so burdensome that it in effect causes the systems to go "underground", making it even harder to uncover money laundering and terrorist financing through alternative remittance.

a. Customer Identification

19. The principle of Know Your Customer ('KYC') has been the backbone of anti-money laundering and counter terrorist financing measures which have been introduced to financial service providers in recent years, and this should also be the case for the MVT service sector. Customer identification requirements in the formal financial sector have had a deterrent effect, causing a shift in money laundering activities to other sectors. FATF Recommendations 4-10 and 12 concern customer identification and record keeping.

- FATF's Recommendation 5 is considered to be the minimum effective level which MVT services should be required to fulfil. The current recommendation sets out that the institution should be "*identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information*". The documents commonly acknowledged and accepted for identification purposes are identity card, passport, drivers' license or social security card. It is important for the credibility of the system that failure to produce an acceptable form of identification will mean that a client will be rejected, the transaction will not be conducted and, under specific circumstances a suspicious transaction report will be made.

- Proof of identity should be required when establishing a business relationship with the MVT service whether the relationship is a short term i.e. a single transaction, or a long term one. Transactions via phone, fax or Internet should only be conducted after customer identification complying with FATF Recommendation 5 has occurred (i.e., a business relationship has already been established). If the client's identification has not been previously established, then the transaction should not be processed.[9]

b. Record Keeping Requirement

20. Investigative agencies need to be able to retrace transactions and identify persons effecting the transactions (i.e. the audit trail) if they are to successfully investigate money laundering and terrorist financing. The requirement for MVT services to maintain records is essential for effective regulation of the field, but it is this area in which the balance between the regulator's needs and the burden on the operator most clearly needs to be struck.

[9] See footnote 3.

- Jurisdictions should consider FATF's Special Recommendation VII on Wire Transfers[10] when developing guidance in this area. This recommendation specifically deals with funds transfers, including those made through MVT services. It should be noted that Special Recommendation VI covers the transmission of "value" as well as money.

- MVT services should comply with FATF Recommendation 10 to maintain, for at least five years, all necessary records on transactions both domestic and international. Jurisdictions should consider setting some minimum requirements for the form in which the records should be kept. Because records associated with MVT transfer services may often be coded and/or difficult to access, jurisdictions should also establish minimum standards for ensuring that they are intelligible and retrievable.

c. Suspicious Transaction Reporting

21. To maintain consistency with the obligations imposed on other financial institutions, jurisdictions should introduce transaction reporting in line with their current reporting requirements for financial institutions.

- Jurisdictions may consider issuing specific guidance as to what may constitute a suspicious transaction to the MVT service industry. Some currently used indicators of suspicious financial activity, such as those found in the FATF's Guidance for Financial Institutions in Detecting Terrorist Financing, are likely to be relevant for money/value transfer service activity. However, particular activities and indicators that are unique to this sector should be further developed.

- The second half of FATF's Special Recommendation VII on Wire Transfers should also be taken into account when developing guidance in this area. For example, operators that receive funds/value should ensure that the necessary originator information is included. The lack of complete originator information may be considered as a factor in assessing whether a transaction is suspicious and, as appropriate, whether it is thus required to be reported to the Financial Intelligence Unit or other competent authorities. If this information is not included, the operator should report suspicious activity to the local FIU or other competent authority if appropriate.

(iv) Compliance Monitoring

22. Regulatory authorities need to monitor the sector with a view to identifying illegal operators and use of these facilities by criminal and terrorist groups. Jurisdictions are encouraged to consider the following options:

- Competent authorities should also be entitled to check on unregistered entities that are suspected to be involved in MVT services. There should be an effective process for using this authority.

- Granting regulatory agencies or supervisory authorities the authority to check the operations of a MVT service and make unexpected visits to operators to allow for the checking of the register's details and the inspection of records. Record keeping practices should be given particular attention.

[10] Text of SRVII: Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain. Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

- Establishing a process of identifying and classifying operators which are considered to be of high risk. In this context, "high risk" means those operators which are considered to be of high risk of being used to carry out money laundering or terrorist financing activities. Jurisdictions are encouraged to give such high risk entities extra attention from supervising authorities.

(v) Sanctions

23. In designing legislation to address this problem, one of the aspects to be considered concerns the sanctions which are available to redress non-compliance. If a MVT service operator is found to be non-compliant with the relevant requirements of the legislation the competent authorities would be expected to sanction the operator. Ideally, jurisdictions should set up a system to employ civil, criminal or administrative sanctions depending on the severity of the offence. For instance, in some cases a warning may initially suffice. However, if a MVT service continues to be in non-compliance, it should receive stronger measures. There should be particularly strong penalties for MVT services and their operators that knowingly act against the law, for example by not registering.

24. To monitor the continued suitability of an individual to conduct a MVT service, jurisdictions are encouraged to put systems into place which would bring any conviction of an operator, shareholder or director following licensing or registration, to the attention of the appropriate authorities. Consideration should be given to defining the type of criminal record which would make the applicant ineligible to be a MVT service provider.

COMBATING THE ABUSE OF NON-PROFIT ORGANISATIONS

International Best Practices

Introduction and definition

1. The misuse of non-profit organisations for the financing of terrorism is coming to be recognised as a crucial weak point in the global struggle to stop such funding at its source. This issue has captured the attention of the Financial Action Task Force (FATF), the G7, and the United Nations, as well as national authorities in many regions. Within the FATF, this has rightly become the priority focus of work to implement Special Recommendation VIII (Non-profit organisations).

2. Non-profit organisations can take on a variety of forms, depending on the jurisdiction and legal system. Within FATF members, law and practice recognise associations, foundations, fund-raising committees, community service organisations, corporations of public interest, limited companies, Public Benevolent Institutions, all as legitimate forms of non-profit organisation, just to name a few.

3. This variety of legal forms, as well as the adoption of a risk-based approach to the problem, militates in favour of a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to protect non-profit organisations **that engage in raising or disbursing funds** for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works" from being misused or exploited by the financiers of terrorism.

Statement of the Problem

4. Unfortunately, numerous instances have come to light in which the mechanism of charitable fundraising – *i.e.*, the collection of resources from donors and its redistribution for charitable purposes – has been used to provide a cover for the financing of terror. In certain cases, the organisation itself was a mere sham that existed simply to funnel money to terrorists. However, often the abuse of non-profit organisations occurred without the knowledge of donors, or even of members of the management and staff of the organisation itself, due to malfeasance by employees and/or managers diverting funding on their own. Besides financial support, some non-profit organisations have also provided cover and logistical support for the movement of terrorists and illicit arms. Some examples of these kinds of activities were presented in the 2001-2002 FATF Report on Money Laundering Typologies[11]; others are presented in the annex to this paper.

Principles

5. The following principles guide the establishment of these best practices:

- The charitable sector is a vital component of the world economy and of many national economies and social systems that complements the activity of the governmental and business sectors in supplying a broad spectrum of public services and improving quality of life. We wish to safeguard and maintain the practice of charitable giving and the strong and diversified community of institutions through which it operates.

[11] Published 1 February 2002 and available at http://www.fatf-gafi.org/FATDocs_en.htm#Trends.

- Oversight of non-profit organisations is a co-operative undertaking among government, the charitable community, persons who support charity, and those whom it serves. Robust oversight mechanisms and a degree of institutional tension between non-profit organisations and government entities charged with their oversight do not preclude shared goals and complementary functions – both seek to promote transparency and accountability and, more broadly, common social welfare and security goals.

- Government oversight should be flexible, effective, and proportional to the risk of abuse. Mechanisms that reduce the compliance burden without creating loopholes for terrorist financiers should be given due consideration. Small organisations that do not raise significant amounts of money from public sources, and locally based associations or organisations whose primary function is to redistribute resources among members may not necessarily require enhanced government oversight.

- Different jurisdictions approach the regulation of non-profit organisations from different constitutional, legal, regulatory, and institutional frameworks, and any international standards or range of models must allow for such differences, while adhering to the goals of establishing transparency and accountability in the ways in which non-profit organisations collect and transmit funds. It is understood as well that jurisdictions may be restricted in their ability to regulate religious activity.

- Jurisdictions may differ on the scope of purposes and activities that are within the definition of "charity," but all should agree that it does not include activities that directly or indirectly support terrorism, including actions that could serve to induce or compensate for participation in terrorist acts.

- The non-profit sector in many jurisdictions has representational, self-regulatory, watchdog, and accreditation organisations that can and should play a role in the protection of the sector against abuse, in the context of a public-private partnership. Measures to strengthen self-regulation should be encouraged as a significant method of decreasing the risk of misuse by terrorist groups.

Areas of focus

6. Preliminary analysis of the investigations, blocking actions, and law-enforcement activities of various jurisdictions indicate several ways in which non-profit organisations have been misused by terrorists and suggests areas in which preventive measures should be considered.

(i) Financial transparency

7. Non-profit organisations collect hundreds of billions of dollars annually from donors and distribute those monies – after paying for their own administrative costs – to beneficiaries. Transparency is in the interest of the donors, organisations, and authorities. However, the sheer volume of transactions conducted by non-profit organisations combined with the desire not to unduly burden legitimate organisations generally underscore the importance of risk and size-based proportionality in setting the appropriate level of rules and oversight in this area.

a. Financial accounting

- Non-profit organisations should maintain and be able to present full program budgets that account for all programme expenses. These budgets should indicate the identity of recipients and how the money is to be used. The administrative budget should also be protected from diversion through similar oversight, reporting, and safeguards.

- Independent auditing is a widely recognised method of ensuring that that accounts of an organisation accurately reflect the reality of its finances and should be considered a best practice. Many major non-profit organisations undergo audits to retain donor confidence, and regulatory authorities in some jurisdictions require them for non-profit organisations. Where practical, such audits should be conducted to ensure that such organisations are not being abused by terrorist groups. It should be noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.

b. Bank accounts:

- It is considered a best practice for non-profit organisations that handle funds to maintain registered bank accounts, keep its funds in them, and utilise formal or registered financial channels for transferring funds, especially overseas. Where feasible, therefore, non-profit organisations that handle large amounts of money should use formal financial systems to conduct their financial transactions. Adoption of this best practice would bring the accounts of non-profit organisations, by and large, within the formal banking system and under the relevant controls or regulations of that system.

(ii) Programmatic verification

8. The need to verify adequately the activities of a non-profit organisation is critical. In several instances, programmes that were reported to the home office were not being implemented as represented. The funds were in fact being diverted to terrorist organisations. Non-profit organisations should be in a position to know and to verify that funds have been spent as advertised and planned.

a. Solicitations

9. Solicitations for donations should accurately and transparently tell donors the purpose(s) for which donations are being collected. The non-profit organisation should then ensure that such funds are used for the purpose stated.

b. Oversight

10. To help ensure that funds are reaching the intended beneficiary, non-profit organisations should ask following general questions:

- Have projects actually been carried out?
- Are the beneficiaries real?
- Have the intended beneficiaries received the funds that were sent for them?
- Are all funds, assets, and premises accounted for?

c. Field examinations

11. In several instances, financial accounting and auditing might be insufficient protection against the abuse of non-profit organisations. Direct field audits of programmes may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including diversion of funds to terrorists. Given considerations of risk-based proportionality, across-the-board examination of all programmes would not be required. However, non-profit organisations should track programme accomplishments as well as finances. Where warranted, examinations to verify reports should be conducted.

d. Foreign operations

12. When the home office of the non-profit organisation is in one country and the beneficent operations take place in another, the competent authorities of both jurisdictions should strive to

exchange information and co-ordinate oversight or investigative work, in accordance with their comparative advantages. Where possible, a non-profit organisation should take appropriate measures to account for funds and services delivered in locations other than in its home jurisdiction.

(iii) Administration

13. Non-profit organisations should be able to document their administrative, managerial, and policy control over their operations. The role of the Board of Directors, or its equivalent, is key.

14. Much has been written about the responsibilities of Boards of Directors in the corporate world and recent years have seen an increased focus and scrutiny of the important role of the Directors in the healthy and ethical functioning of the corporation. Directors of non-profit organisations, or those with equivalent responsibility for the direction and control of an organisation's management, likewise have a responsibility to act with due diligence and a concern that the organisation operates ethically. The directors or those exercising ultimate control over a non-profit organisation need to know who is acting in the organisation's name – in particular, responsible parties such as office directors, plenipotentiaries, those with signing authority and fiduciaries. Directors should exercise care, taking proactive verification measures whenever feasible, to ensure their partner organisations and those to which they provide funding, services, or material support, are not being penetrated or manipulated by terrorists.

15. Directors should act with diligence and probity in carrying out their duties. Lack of knowledge or passive involvement in the organisation's affairs does not absolve a director – or one who controls the activities or budget of a non-profit organisation – of responsibility. To this end, directors have responsibilities to:

- The organisation and its members to ensure the financial health of the organisation and that it focuses on its stated mandate.
- Those with whom the organisation interacts, like donors, clients, suppliers.
- All levels of government that in any way regulate the organisation.

16. These responsibilities take on new meaning in light of the potential abuse of non-for-profit organisations for terrorist financing. If a non-profit organisation has a board of directors, the board of directors should:

- Be able to identify positively each board and executive member;
- Meet on a regular basis, keep records of the decisions taken at these meetings and through these meetings;
- Formalise the manner in which elections to the board are conducted as well as the manner in which a director can be removed;
- Ensure that there is an annual independent review of the finances and accounts of the organisation;
- Ensure that there are appropriate financial controls over program spending, including programs undertaken through agreements with other organisations;
- Ensure an appropriate balance between spending on direct programme delivery and administration;
- Ensure that procedures are put in place to prevent the use of the organisation's facilities or assets to support or condone terrorist activities.

Oversight bodies

17. Various bodies in different jurisdictions interact with the charitable community. In general, preventing misuse of non-profit organisations or fundraising organisations by terrorists has not been a historical focus of their work. Rather, the thrust of oversight, regulation, and accreditation to date has been maintaining donor confidence through combating waste and fraud, as well as ensuring that

government tax relief benefits, where applicable, go to appropriate organisations. While much of this oversight focus is fairly easily transferable to the fight against terrorist finance, this will also require a broadening of focus.

18. There is not a single correct approach to ensuring appropriate transparency within non-profit organisations, and different jurisdictions use different methods to achieve this end. In some, independent charity commissions have an oversight role, in other jurisdictions government ministries are directly involved, just to take two examples. Tax authorities play a role in some jurisdictions, but not in others. Other authorities that have roles to play in the fight against terrorist finance include law enforcement agencies and bank regulators. Far from all the bodies are governmental – private sector watchdog or accreditation organisations play an important role in many jurisdictions.

(i) Government Law Enforcement and Security officials

19. Non-profit organisations funding terrorism are operating illegally, just like any other illicit financier; therefore, much of the fight against the abuse of non-profit organisations will continue to rely heavily on law enforcement and security officials. Non-profit organisations are not exempt from the criminal laws that apply to individuals or business enterprises.

- Law enforcement and security officials should continue to play a key role in the combat against the abuse of non-profit organisations by terrorist groups, including by continuing their ongoing activities with regard to non-profit organisations.

(ii) Specialised Government Regulatory Bodies

20. A brief overview of the pattern of specialised government regulation of non-profit organisations shows a great variety of practice. In England and Wales, such regulation is housed in a special Charities Commission. In the United States, any specialised government regulation occurs at the sub-national (state) level. GCC member countries oversee non-profit organisations with a variety of regulatory bodies, including government ministerial and intergovernmental agencies.

- In all cases, there should be interagency outreach and discussion within governments on the issue of terrorist financing – especially between those agencies that have traditionally dealt with terrorism and regulatory bodies that may not be aware of the terrorist financing risk to non-profit organisations. Specifically, terrorist financing experts should work with non-profit organisation oversight authorities to raise awareness of the problem, and they should alert these authorities to the specific characteristics of terrorist financing.

(iii) Government Bank, Tax, and Financial Regulatory Authorities

21. While bank regulators are not usually engaged in the oversight of non-profit organisations, the earlier discussion of the importance of requiring charitable fund-raising and transfer of funds to go through formal or registered channels underscores the benefit of enlisting the established powers of the bank regulatory system – suspicious activity reporting, know-your-customer (KYC) rules, etc – in the fight against terrorist abuse or exploitation of non-profit organisations.

22. In those jurisdictions that provide tax benefits to charities, tax authorities have a high level of interaction with the charitable community. This expertise is of special importance to the fight against terrorist finance, since it tends to focus on the financial workings of charities.

- Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIUs) to the maximum extent possible. Though such tax-related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organisations by terrorist groups or supporters is shared as appropriate.

(iv) Private Sector Watchdog Organisations

23. In the countries and jurisdictions where they exist, the private sector watchdog or accreditation organisations are a unique resource that should be a focal point of international efforts to combat the abuse of non-profit organisations by terrorists. Not only do they contain observers knowledgeable of fundraising organisations, they are also very directly interested in preserving the legitimacy and reputation of the non-profit organisations. More than any other class of participants, they have long been engaged in the development and promulgation of "best practices" for these organisations in a wide array of functions.

24. Jurisdictions should make every effort to reach out and engage such watchdog and accreditation organisations in their attempt to put best practices into place for combating the misuse of non-profit organisations. Such engagement could include a dialogue on how to improve such practices.

Sanctions

25. Countries should use existing laws and regulations or establish any such new laws or regulations to establish effective and proportionate administrative, civil, or criminal penalties for those who misuse charities for terrorist financing.

TYPOLOGIES OF TERRORIST MISUSE OF NON-PROFIT ORGANISATIONS

Annex

Example 1: Non-profit front organisation

1. In 1996, a number of individuals known to belong to the religious extremist groups established in the south-east of an FATF country (Country A) convinced wealthy foreign nationals, living for unspecified reasons in Country A, to finance the construction of a place of worship. These wealthy individuals were suspected of assisting in the concealment of part of the activities of a terrorist group. It was later established that "S", a businessman in the building sector, had bought the building intended to house the place of worship and had renovated it using funds from one of his companies. He then transferred the ownership of this building, for a large profit, to Group Y belonging to the wealthy foreigners mentioned above.

2. This place of worship intended for the local community in fact also served as a place to lodge clandestine "travellers" from extremist circles and collect funds. For example, soon after the work was completed, it was noticed that the place of worship was receiving large donations (millions of dollars) from other wealthy foreign businessmen. Moreover, a Group Y worker was said to have convinced his employers that a "foundation" would be more suitable for collecting and using large funds without attracting the attention of local authorities. A foundation was thus reportedly established for this purpose.

3. It is also believed that part of "S's" activities in heading a multipurpose international financial network (for which investments allegedly stood at USD 53 million for Country A in 1999 alone) was to provide support to a terrorist network. "S" had made a number of trips to Afghanistan and the United States. Amongst his assets were several companies registered in Country C and elsewhere. One of these companies, located in the capital of Country A, was allegedly a platform for collecting funds. "S" also purchased several buildings in the south of Country A with the potential collusion of a notary and a financial institution.

4. When the authorities of Country A blocked a property transaction on the basis of the foreign investment regulations, the financial institution's director stepped in to support his client's transaction and the notary presented a purchase document for the building thus ensuring that the relevant authorisation was delivered. The funds held by the bank were then transferred to another account in a bank in an NCCT jurisdiction to conceal their origin when they were used in Country A.

5. Even though a formal link has not as yet been established between the more or less legal activities of the parties in Country A and abroad and the financing of terrorist activities carried out under the authority a specific terrorist network, the investigators suspect that at least part of the proceeds from these activities have been used for this purpose.

VIII. Example 2: Fraudulent solicitation of donations

6. One non-profit organisation solicited donations from local charities in a donor region, in addition to fund raising efforts conducted at its headquarters in a beneficiary region. This non-profit organisation falsely asserted that the funds collected were destined for orphans and widows. In fact, the finance chief of this organisation served as the head of organised fundraising for Usama bin Laden. Rather than providing support for orphans and widows, funds collected by the non-profit organisation were turned over to al-Qaida operatives.

Example 3: Branch offices defraud headquarters

7. The office director for a non-profit organisation in a beneficiary region defrauded donors from a donor region to fund terrorism. In order to obtain additional funds from the headquarters, the branch office padded the number of orphans it claimed to care for by providing names of orphans that did not exist or who had died. Funds then sent for the purpose of caring for the non-existent or dead orphans were instead diverted to al-Qaida terrorists.

8. In addition, the branch office in a beneficiary region of another non-profit organisation based in a donor region provided a means of funnelling money to a known local terrorist organisation by disguising funds as intended to be used for orphanage projects or the construction of schools and houses of worship. The office also employed members of the terrorist organisations and facilitated their travel

IX. Example 4: Aid worker's Misuse of Position

9. An employee working for an aid organisation in a war-ravaged region used his employment to support the ongoing activities of a known terrorist organisation from another region. While working for the aid organisation as a monitor for work funded in that region, the employee secretly made contact with weapons smugglers in the region. He used his position as cover as he brokered the purchase and export of weapons to the terrorist organisation.

ANNEX C

Compliance with the FATF Eight Special Recommendations: 2002-2003 Self-Assessment on Terrorist Financing

Chart (a)

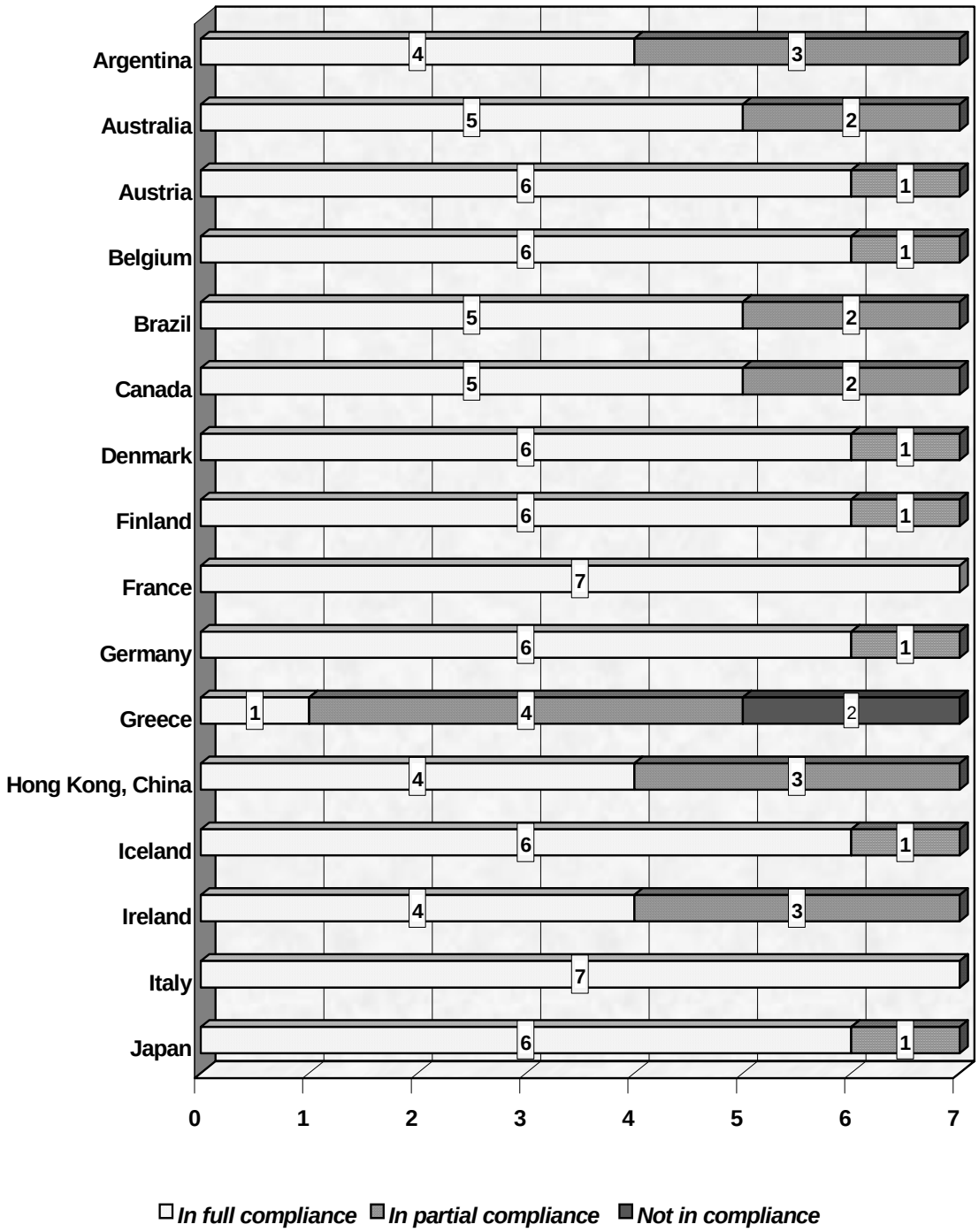
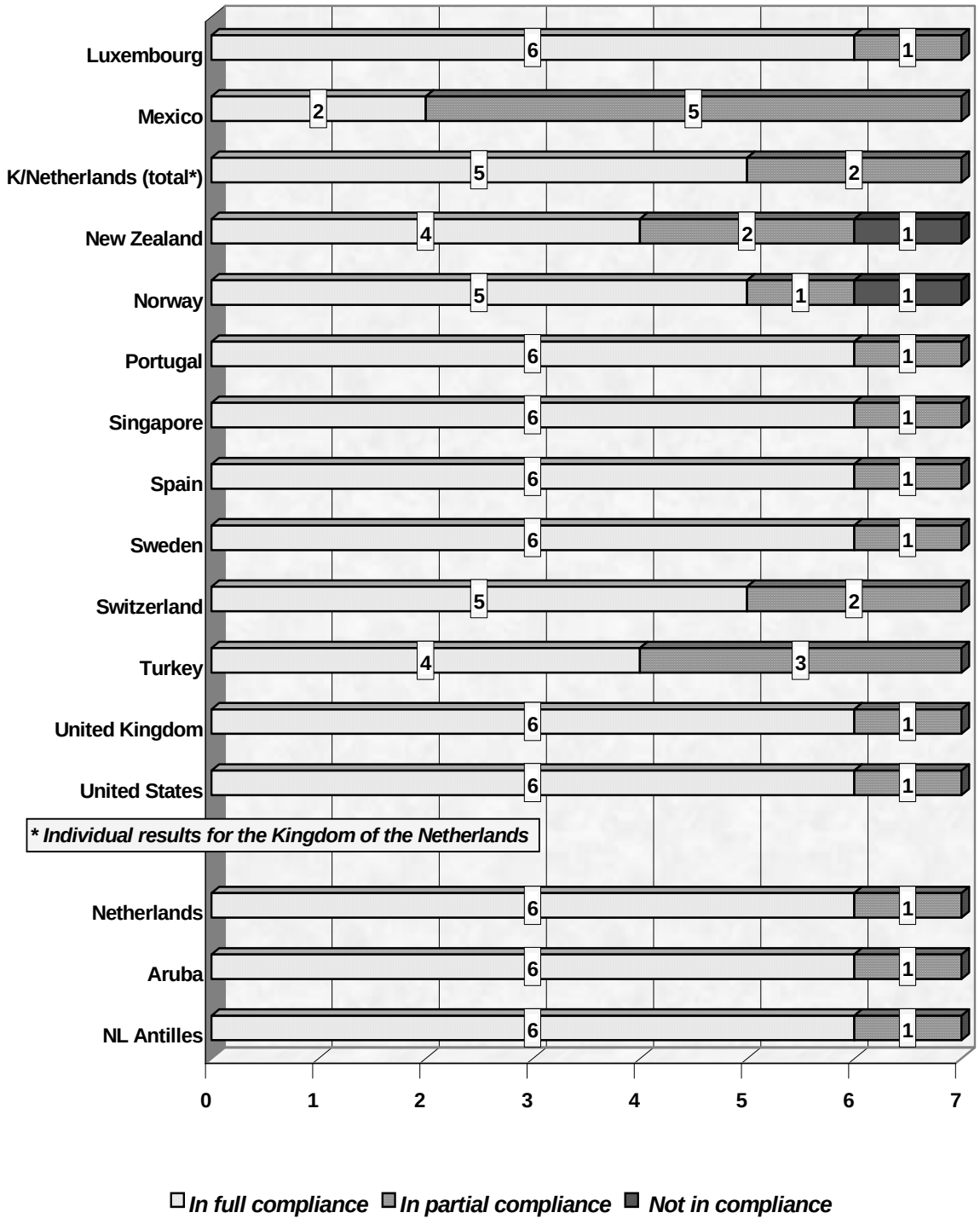


Chart (b)

Self-Assessement against the FATF Special Recommendations on Terrorist Financing 2002-2003

(Special Recommendations 1-7)



COMPLIANCE WITH THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING 2002-2003 SELF-ASSESSMENT EXERCISE

Explanatory Note

General

1. As part of the Plan of Action adopted by the FATF at its October 2001 extraordinary Plenary meeting, the FATF issued a set international standards to combat terrorist financing – the Eight Special Recommendations. In order to assess the level of implementation called for in the Eight Special Recommendations a self-assessment exercise for FATF members was initiated in December 2001. The self-assessment exercise determines – based mainly on information provided by each member jurisdiction – what steps have been taken to implement the Special Recommendations. The results of the initial self-assessment exercise for FATF members were published in the FATF-XIII annual report 2001-2002. Subsequent self-assessment exercises are then designed to establish a record of members' progress in implementing the Special Recommendations.

2. During 2002-2003 the FATF issued interpretative notes on Special Recommendations VI and VII, the publication of these papers ensures that appropriate standards are set and informs the assessment criteria. In assessing compliance with Special Recommendation VIII, since the publication of a best practices paper in October 2002, the FATF continues to consider the best way to accomplish this task. It is likely that the FATF will continue to examine appropriate assessment criteria for Special Recommendation VIII in the context of developing further guidance. This explanatory note provides detail to the accompanying charts and comments on each FATF members' current level of compliance with seven of the eight Special Recommendations.

Notes on specific Results

3. On the basis of the information provided by FATF members, two jurisdictions (France and Italy) are assessed as being in full compliance with seven of the Special Recommendations[1] that have been assessed. Details of the current compliance status for other FATF members are as follows, again, according to information from FATF members themselves.

Argentina is in full compliance with four of the Special Recommendations (SRs) and is in partial compliance with three. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1]. For SR II, although terrorist financing is a predicate offence for money laundering, it has not yet been criminalised as an autonomous offence. For SR VI, informal money/value transfer (IMVT) systems are not subject to relevant FATF Recommendations, and there are no sanctions should IMVT systems fail to comply with the applicable FATF Recommendations.

Australia is in full compliance with five SRs and is in partial compliance with SR VI, as IMVT services are not yet required to be licensed or registered. For SR VII, transfer services, which are not Australian financial institutions but operate in Australia, do not yet meet all the necessary measures.

Austria is in full compliance with six of the SRs. For SR VII, it is in partial compliance because it has not yet implemented necessary measures for MVT services.

Belgium is in full compliance with six of the seven SRs. It is in partial compliance with SR I, because certain United Nations instruments have not yet been fully implemented [Note 1].

[1] Information on the Eight Special Recommendations on Terrorist Financing can be found on the FATF website at: http://www.fatf-gafi.org/SRecsTF_en.htm

Brazil is in full compliance with five SRs. It is in partial compliance with SR I because certain United Nations instruments have yet been fully implemented [Note 1] and with SR II because the financing of terrorism, terrorist acts and terrorist organisations is not a predicate offence for money laundering.

Canada is in full compliance with five of the SRs. It is in partial compliance with SR VI, as there are no specific provisions that require persons or legal entities providing MVT services to register or be licensed. Natural or legal persons who conduct MVT services without proper authorisation are not subject to sanctions. It is in partial compliance with SR VII because it has not yet implemented all necessary measures.

Denmark is in full compliance with six SRs. It is in partial compliance with SR VI, as there is no specific competent authority to supervise or monitor MVT services (including IMVT services).

Finland is in full compliance with six SRs. It is in partial compliance with SR VII because it has not yet implemented necessary measures for MVT services.

Germany is in full compliant with six SRs. It is in partially compliant with SR I because certain United Nations instruments have not yet been fully implemented [Note 1].

Greece is in full compliance with one SR and in partial compliance with five. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1]. For SR III, as there are no provisions to permit the freezing, seizing and confiscation of all types of terrorist property. And for SR V mutual legal assistance or other mechanisms for exchanging information to respond to inquiries relating to terrorist financing are required. Measures are also necessary to deny safe haven to those involved in the financing of terrorism. There are no provisions that prevent refusal of extradition requests because of political motivation. Financial institutions do not yet fully meet the requirements for Special Recommendation VII. Greece is in non-compliance with SR II and IV as none of the necessary measures have been implemented.

Hong Kong, China is in full compliance with four SRs and in partial compliance with three. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1]. For SR III, there are provisions to freeze, seize and confiscate terrorist funds, but the provisions are not yet to come into operation. Legislative amendments are also being made to extend the scope to cover terrorist properties as well. For SRV, there are no provisions that prevent refusal of extradition requests because of political motivation.

Iceland is in full compliance with six SRs. For SR II, the financing of terrorism is not a predicate offence for money laundering. It is also not an offence if the terrorist act is committed in another State.

Ireland is in full compliance with four SRs and is in partial compliance with three. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1]. For SR VI, MVT services are not required to be licensed or registered and are not subject to relevant FATF Recommendations. There is no authority to ensure MVT services comply with the relevant FATF Recommendations and persons or legal entities which operate MVT services (including IMVT systems) without proper authorisation are not subject to sanctions.

Japan is in full compliance with six SRs. It is in partial compliance with SR VII because it has not yet implemented all necessary measures.

Luxembourg is in full compliance with six SRs. It is in partial compliance with SR I as the United Nations 1999 Convention for the Suppression of the Financing of Terrorist Finance has not yet been ratified or implemented [Note 1].

Mexico is in full compliance with two SRs and is in partially compliant with five. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1]. For SR II, the financing of

terrorism is not a criminal offence although it is a predicate offence for money laundering. For SR IV, MVT systems do not have a reporting obligation where funds are suspected of being linked to terrorism [Note 2]. For SR VI, MVT systems are not subject to relevant FATF Recommendations, there is no specific authority to ensure MVT systems comply with the relevant FATF Recommendations and to sanction them should they fail to comply. For SR VII Mexico has not yet implemented necessary measures for MVT services.

.

Kingdom of the Netherlands consists of three components (the Netherlands, Aruba and the Netherlands Antilles). The assessment made for the Kingdom combines the results from the three parts. In this combined assessment, the Kingdom is in compliance with five SRs. The results from the three individual components of the Kingdom of the Netherlands are as follows:

- ***Netherlands*** is in full compliance with six SRs. It is in partial compliance with SR VII because it has not yet implemented all necessary measures.

- ***Aruba*** is in full compliance with six of the seven SRs and partially compliant with one. For SR I, it is in partial compliance, as certain United Nations instruments have not yet been fully implemented [Note 1].

- ***Netherlands Antilles*** is in full compliance with six SRs. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1].

New Zealand is in full compliance with four SRs. It is in partial compliance with SRs I and VI. For SR I, certain United Nations instruments have not yet been fully implemented [Note 1]. For SR VI, MVT (including IMVT systems) are not required to be licensed or registered, there is no specific competent authority to oversee any licensing or registration regime and entities which operate MVT services (including IMVT systems) without proper authorisation are not subject to sanctions. New Zealand is in non-compliance with SR VII, as it has not yet implemented any of the necessary measures.

Norway is in full compliance with five SRs. It is partially compliant with SR VI because MVT services are not subject to relevant FATF Recommendations and there is no specific competent authority to oversee any licensing or registration regime and entities which operate MVT services (including IMVT systems). It is in non-compliance with SR VII, because it has not yet implemented any of the necessary measures.

Portugal is in full compliance with six SRs and is in partial compliance with one. For SR VII, certain categories of financial institutions are not yet subject to relevant requirements.

Singapore is in full compliance with six SRs. It is in partial compliance with SR VII because it has not yet implemented certain of the necessary measures.

Spain is compliant with six SRs. It is in partial compliance with SR VII, because it has not yet extended full measures to MVT service

Sweden is compliant with six SRs. It is in partial compliance with SR VII because it has not yet implemented necessary measures for MVT services.

Switzerland is compliant with five SRs. It is partially complaint with SR I, as certain United Nations instruments have not yet been fully implemented [Note 1]. For SR VII, Switzerland has not yet implemented necessary measures for MVT services.

Turkey is compliant with four SRs and partially compliant with three. For SR I, it has not yet implemented the United Nations 1999 Convention for the Suppression of the Financing of Terrorism

[Note 1]. For SR II, it is in partial compliance because terrorist financing is not a predicate offence for money laundering. For SR III, there are no provisions to seize and confiscate terrorist property**.**

United Kingdom is compliant with six SRs. For SR VII the United Kingdom has not yet implemented all necessary measures for MVT services.

United States is compliant with six SRs. It is partially compliant with SR IV, insurance companies are not obligated to report when funds are suspected of being linked to terrorism. A proposed rule, when it becomes final later in 2003, will extend the necessary obligation to insurance companies.

Note 1

The relevant United Nations instruments in relation to SR I are the United Nations 1999 Convention for the Suppression of the Financing of Terrorism and United Nations Security Council Resolutions 1267 (1999), 1269 (1999), 1333 (2000), 1373 (2001) and 1390 (2002)[2].

Note 2

References to "financial institutions" in relation to SR VI refer to both banks and non-bank financial institutions (NBFIs). NBFIs include as a minimum: bureaux de change, stockbrokers, insurance companies and money remittance/transfer service

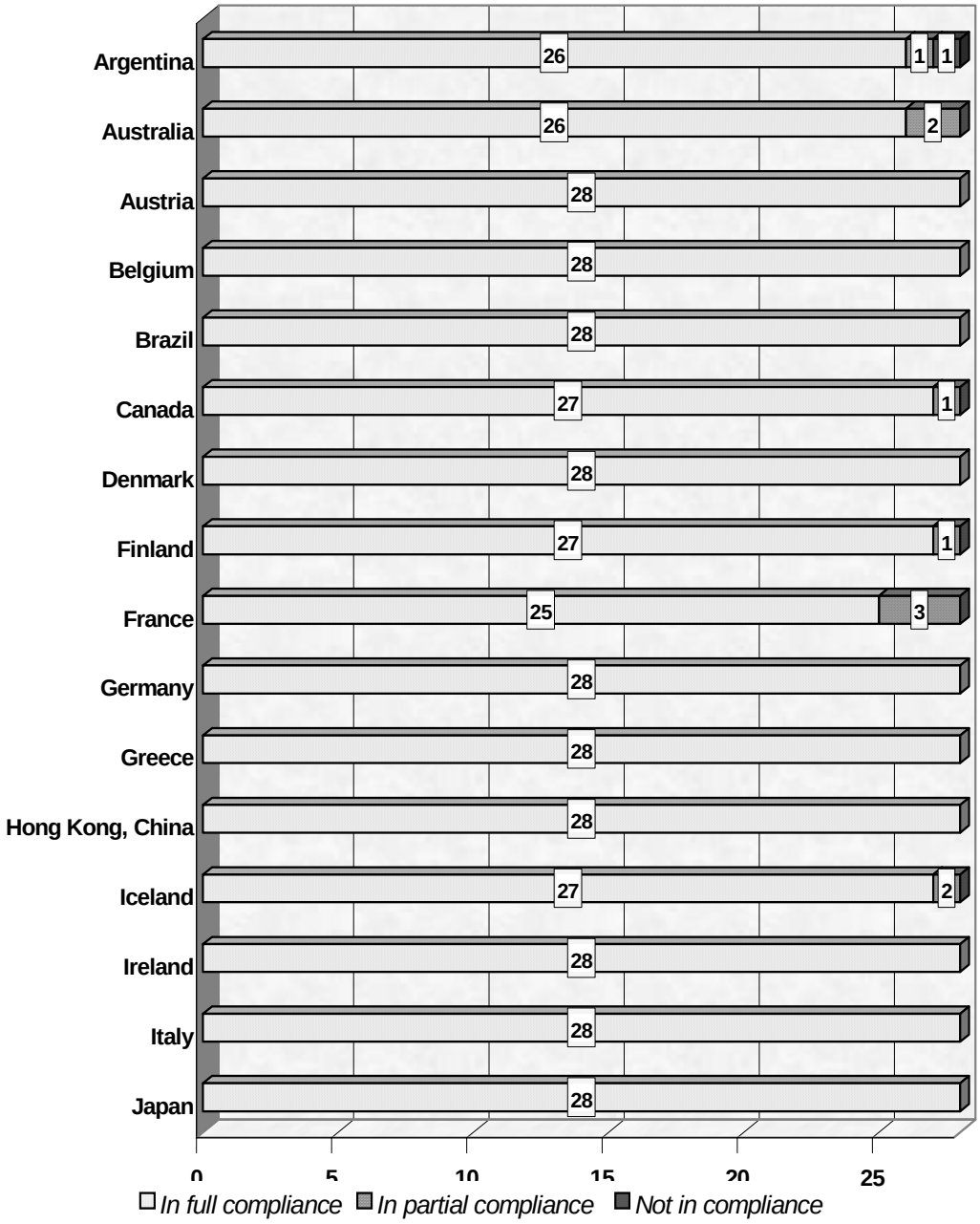
[2] The provisions of UNSCR 1390 (2002) have been extended by UNSCR 1455 (2003).

ANNEX D

COMPLIANCE WITH THE 1996 FATF FORTY RECOMMENDATIONS: 2002-2003 SELF-ASSESSMENT

Chart (a)

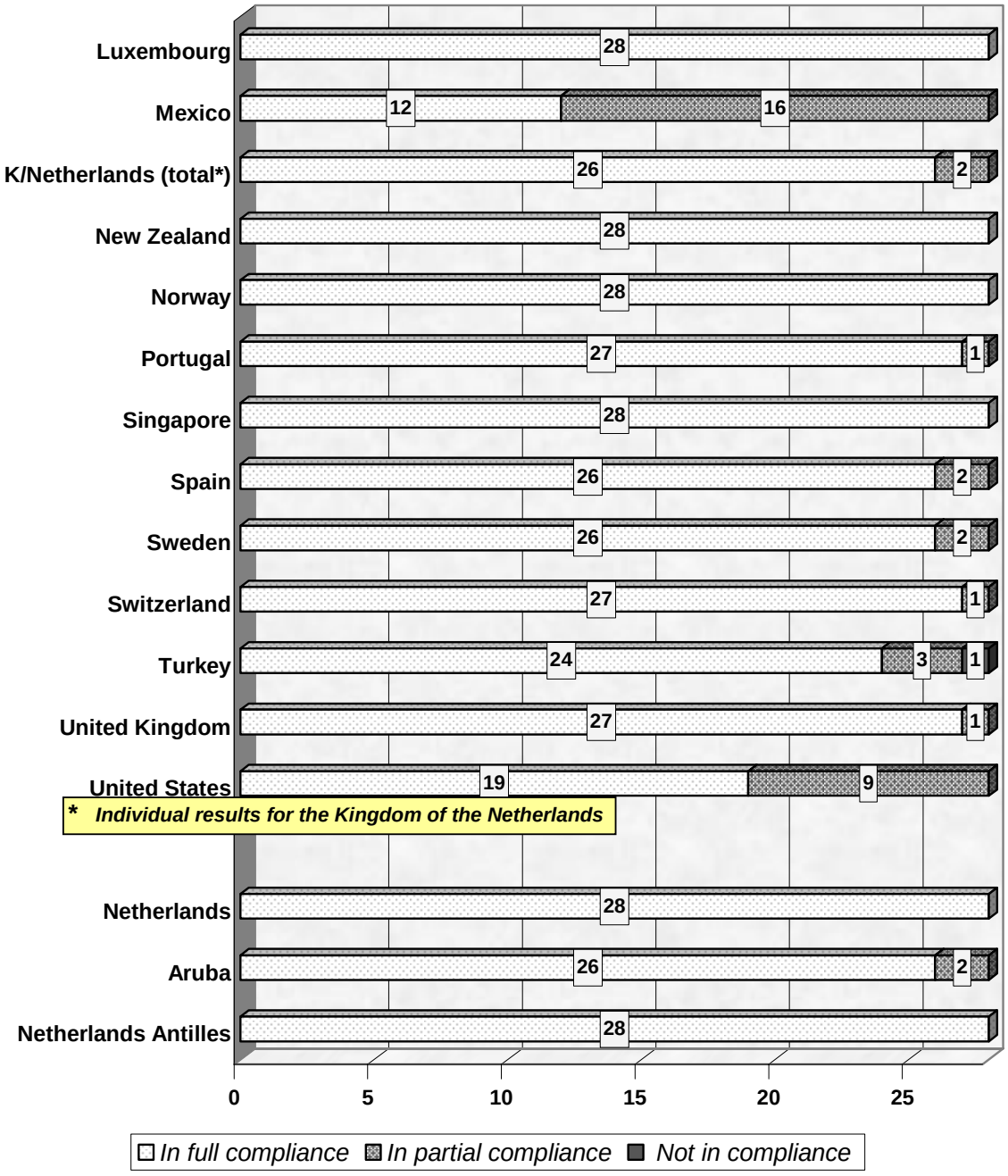
Compliance with FATF 40 Recommendations
2002-2003 Self-Assessment Survey*
(for 28 Recommendations requiring specific action)



SEE EXPLANATORY NOTE STARTING ON PAGE 3

Chart (b)

Compliance with FATF 40 Recommendations
2002-2003 Self-Assessment Survey*
(for the 28 Recommendations requiring specific action)



* *Individual results for the Kingdom of the Netherlands*

Netherlands 28
Aruba 26 2
Netherlands Antilles 28

****SEE EXPLANATORY NOTE STARTING ON PAGE 3***

COMPLIANCE WITH THE FATF 40 RECOMMENDATIONS 2002-2003 SELF-ASSESSMENT SURVEY

Explanatory Note

General

1. The FATF self-assessment exercise is designed to establish an annual record of FATF members' progress in implementing the Recommendations. It seeks to determine – based mainly on information provided by each jurisdiction – what steps have been taken to implement the Recommendations during a particular year. While implementation of particular measures is a critical step in developing a comprehensive anti-money laundering system, self-assessment results cannot be interpreted by themselves as the measure of the effectiveness of any individual anti-money laundering system. Within the FATF, the mutual evaluation process was created as the primary mechanism for examining and judging the progress of FATF members in implementing anti-money laundering measures and for determining the overall effectiveness of such measures. To obtain a complete picture for any FATF jurisdiction, the summaries of their individual mutual evaluations should be consulted.[1]

2. The self-assessment process focuses on the implementation of key legal, financial and international co-operation measures as related to the 28 FATF Recommendations requiring specific action.[2] In the financial area, FATF members were judged on whether they had implemented measures both for banks and for four main categories of non-bank financial institutions (bureaux de change, stockbrokers, insurance companies and money remittance/transfer companies). Combining these five types of financial institutions into a single category has increased the focus on uniform application of anti-money laundering measures in the non-bank financial institution area.

Notes on Specific Results

3. On the basis of the information provided by FATF members, the following jurisdictions were assessed for 2002-2003 as having fully implemented the 28 FATF Recommendations requiring specific action: Austria; Belgium; Brazil; Denmark; Germany; Greece; Hong Kong, China; Ireland; Italy; Japan; Luxembourg; New Zealand; Norway and Singapore.

4. Details on the compliance status and changes during the past year in FATF members are as follows (again on the basis of information provided by the jurisdictions themselves):

Argentina is in full compliance with **26** Recommendations Argentina is in partial compliance with R. 38 because of limitations in its seizure and confiscation measures. R. 20 has not been implemented yet.

Australia is in full compliance with **26** Recommendations. Enactment of the Proceeds of Crime Act in 2002, which came into force on 1 January 2003, provides for a non-conviction based forfeiture scheme. Under this legislation, it is now possible to restrain and forfeit instruments intended for use in the commission of an offence or in connection with the commission of an offence. Australia is now in full compliance with R. 7. It is at less than full compliance with R. 19 and 20 because there are no formal obligations imposed on financial institutions regarding these measures, although it is recognised that the measures are in place on a voluntary basis.[3]

---

1 These summaries can be found in the FATF Annual Reports for the year in which a particular evaluation was conducted. The summaries may also be consulted through the FATF website at the following address: http://www.fatf-gafi.org/Members_en.htm.

2 The Recommendations requiring specific action are: Recommendations 1-5, 7, 8, 10-12, 14-21, 26-29, 32-34, 37, 38 and 40. The text of the Forty Recommendations may be consulted at the following website address: http://www.fatf-gafi.org/40Recs_en.htm.

3 Australia considers itself to be in full compliance with R. 19 and 20.

Austria is now in full compliance with **28** Recommendations. As reported previously, Austria enacted legislation in November 2000 that, when its provisions came fully into force, effectively eliminated anonymous passbooks. No new anonymous passbooks have been permitted since enactment of the legislation. On 1 July 2002, the last part of the legislation came into force. From that point, any movements from or to an anonymous passbook have required identification of the holder. Any withdrawals from such passbooks containing EUR 15,000 or more must be reported by the credit institution to the Austrian FIU. Additionally, the transfer or acquisition of anonymous passbooks is now prohibited and subject to administrative sanctions. While anonymous passbooks continue to exist in the strict legal sense, their anonymity has effectively been eliminated. Austria is now in compliance with R. 10.

Canada is in full compliance with **27** Recommendations. Canada remains in partial compliance with R. 29 because it has not yet extended certain measures of the Recommendation to bureaux de change or money transmitters.[4]

Finland is in full compliance with **27** Recommendations. It has not yet extended certain measures under R. 29 to bureaux de change or money remitters; therefore, it is in partial compliance with this Recommendation.

France is in full compliance with **25** Recommendations. It does not have a specific screening requirement for the employees of financial institutions and is thus in partial compliance with R. 19. It has a system in place to communicate guidance on suspicious transaction reporting for financial institutions under the supervision of the French Banking Commission, however no similar system for other financial institutions. It is therefore now in partial compliance with R. 28. France is in partial compliance with R. 33 because it may not provide mutual legal assistance when the intentional element of the money laundering offence is negligence.

Iceland is in full compliance with **27** Recommendations. The provisions of R. 28 have not been fully implemented; therefore, Iceland is in partial compliance with this Recommendation.

Mexico is in full compliance with **12** Recommendations. It is in partial compliance with R. 8, 10-12, 14-21, 26, 28 and 29 due to the fact that it has not extended necessary anti-money laundering measures to money remitters. On 1 June 2001, the Mexican Congress enacted modifications to it anti-money laundering laws that extend relevant requirements to money transmitters. These new measures have not yet come into effect through implementing legislation. With regard to R. 38, seizure and confiscation measures may only be applied against the actual proceeds or property derived from crime and not property or assets of corresponding value. Mexico is therefore in partial compliance with this Recommendation.

The Kingdom of the Netherlands consists of three components (Netherlands, Aruba and Netherlands Antilles). The assessment made for the Kingdom combines the results from the three parts. In this combined assessment, the Kingdom is in full compliance with **26** Recommendations. The results for the individual components are as follows:

- *The Netherlands* is in full compliance with **28** Recommendations. Enactment of the Law on Money Services on 28 June 2002 brought money remitters under the supervision of the Central Bank of the Netherlands. Therefore, the Netherlands now complies with R. 19 for all key financial institutions.

- *Aruba* is in full compliance with **26** Recommendations. It is in partial compliance with R. 21 because it has not extended certain provisions of the Recommendation to all categories of non-

[4] The full range of non-bank financial institutions for the self-assessment process includes bureaux de change, stockbrokers, insurance companies and money remitters/transfer companies.

bank financial institutions. Aruban Parliament has enacted a law which makes it possible for the Aruban FIU to exchanges information related to unusual transactions reports with other jurisdiction without treaty. Aruba will be in full compliance with R. 32 when this new law comes into effect in July 2003.

- *The Netherlands Antilles* is in full compliance with **28** Recommendations. As of July 2002, missing coverage of money remitters was resolved through the establishment of formal "Admission Requirements for Money Transfer Companies Operating in the Netherlands Antilles". Additional, requirements were imposed on through guidelines that came into effect in June 2003. The Netherlands Antilles are therefore now in full compliance with R. 19 and 29 with regard to money remitters.

Portugal is in full compliance with **27** Recommendations. It is in partial compliance with R. 33 because it may not provide mutual legal assistance that involves coercive measures when the intentional element of the money laundering offence is negligence.

Singapore is in now full compliance with **28** Recommendations. The provisions of R. 19 apply to all categories of non-bank financial institutions; therefore, Singapore is in full compliance with this Recommendation.

Spain is in full compliance with **26** Recommendations. Suspicious transaction reporting guidelines have not been issued for bureaux de change; therefore, Spain is in partial compliance with R. 28. With regard to R. 38, Spain is in partial compliance because of limitations in its seizure and confiscation measures.

Sweden is in full compliance with **26** Recommendations. It has not applied provisions of R. 29 to money transmitters and is therefore in partial compliance with this Recommendation. It is at less than full compliance with R. 19 because there are no formal obligations imposed on financial institutions regarding screening procedures for employees, although institutions do this in practice.

Switzerland is in full compliance with **27** Recommendations. It is in partial compliance with R. 1 because it has not yet formally ratified the 1988 *UN Convention against the Illicit Traffic in Narcotics and Psychotropic Substances*. It should be noted, however, that the relevant legislative measures to counter money laundering have been enacted into Swiss law.

Turkey is in full compliance with **24** Recommendations. It is at less than full compliance with R. 19 because some of the necessary provisions of this Recommendation have not been extended to stockbrokers, insurance companies or money remitters. It is also at less than full compliance with R. 33 because it may not provide mutual legal assistance when the intentional element of the money laundering offence is negligence or "should have known standard". Turkey has not yet implemented R. 16 and only partially implemented R. 20 (that is some requirements of this Recommendation apply to banks).

The **United Kingdom** is in full compliance with **27** Recommendations. It is in partial compliance with R. 19 because screening procedures for employees of bureaux de change and money remitters have not been implemented.

The **United States** is in full compliance with **19** Recommendations. Since last year, the US has implemented final rules that impose the requirements of R. 14, 15, 28 and 29 on bureaux de change and money transmitters. The US remains in partial compliance with R. 8, 10-12, 14, 15, 19-20 and 26 due to the fact that it has not extended full anti-money laundering measures to insurance companies. The USA PATRIOT Act, signed into law in October 2001, authorises the US to impose far reaching measures to protect the financial system from money laundering and terrorist financing. A new rule proposed in 2002 deals with implementing relevant measures within the insurance industry. When this

rule is issued in final form, the US will likely reach full compliance with remaining FATF Recommendations.

ANNEX E

SUMMARIES OF MUTUAL EVALUATIONS UNDERTAKEN BY THE COUNCIL OF EUROPE MONEYVAL COMMITTEE

Andorra

1. The Principality of Andorra is the eighth country evaluated by MONEYVAL (PC-R-EV) as part of the Committee's second evaluation round. A team of MONEYVAL evaluators, assisted by two GAFI evaluators and accompanied by two members of the MONEYVAL Secretariat, visited Andorra La Vella for 4 days (4-7 March 2002). Beforehand, they had received detailed replies to the mutual evaluation questionnaire from the Andorran Government. The aim of the present evaluation is to check on developments since the first evaluation round (March 1999) and assess the overall effectiveness of Andorra's anti-money laundering system in practice.

2. According to the Andorran authorities, most of the proceeds from money laundering still come from drugs- trafficking in other countries, and this makes it hard to prove their unlawful origin. There is also some "small-scale trafficking" - mainly linked with own consumption – in Andorra itself. Otherwise, fraud, counterfeiting of currency, corruption and smuggling, often involving organised gangs, are still considered the major potential sources, though at the scale of the country. The proceeds of smuggling are still not regarded as money-laundering, although cigarette smuggling is now a criminal offence and carries corresponding penalties.

3. As compared with the first evaluation round, people setting out to launder money try to bring it into Andorra with the help of nationals or residents exercising a genuine activity in the country. A special effort has been made to train bank staff not to accept sums brought in cash from other countries, and intended for immediate re-transfer abroad, for deposit in Andorran accounts.

4. In the light of the present report, MONEYVAL (PC-R-EV) welcomes the progress made by Andorra since the first evaluation round. Specifically, adoption of the 2000 Act, ratification of the Strasbourg and Vienna Conventions and the establishment of the UPB are all signs of the Andorran Government's genuine desire to bring in an effective policy to curb money laundering.

5. The new Act of December 2000 replaces the 1995 Act and contains a number of important innovations. It establishes the Andorran Financial Information Unit (UPB) and gives it the powers it needs to do its job. The Regulations on the UPB of 27 March 2002 have been amended and adopted, in the form of a Decree approving the Regulation contained in the Act of December 2000. The Act makes the concept of "suspicion" more flexible. Rational indications, relating to "standard" offences in the Penal Code, are no longer required - simple suspicion is enough. The Act extends the list of professions and activities subject to special notification requirements and vigilance in connection with anti-laundering measures. These must identify all their clients. It also introduces a coherent system for prevention, monitoring and notification of suspect or unusual transactions, and provides for consciousness-raising and training programmes for individuals and legal entities subject to the requirements of the Act.

6. The Act specifies procedures for international co-operation and facilitates confiscation and provisional measures, particularly at the request of foreign authorities. The revised Code of Criminal Procedure also provides for important new measures, making it possible to step up the fight against crimes which generate money for laundering, i.e. infiltrators and supervised deliveries.

7. Concerning implementation of the Act, MONEYVAL notes that anti-laundering training has been organised on a vast scale for most of the financial sector. There is also very extensive co-operation between the Andorran police, the Spanish Guardia Civil and police forces in other countries. The UPB started work recently, but has already sent intermediaries technical guidelines on transactions which are likely to involve money- laundering. It is co-operating with its French (TRACFIN) and Spanish (SEPBLANC) counterparts, and has established contacts with other members

of the Egmont Group1 (including the CTIF in Belgium and the SICFFIN in Monaco). However, owing to its recent establishment, it had not yet conducted any inspections at the time of the visit. The evaluation team gleaned no further information regarding the practical feasibility of carrying out such inspections with limited staff. The UPB still had no adequate indicators, allowing it to measure the level of effectiveness, diligence and goal-achievement, and gauge the possible effects of its activities.

8. The system for the notification of suspect or unusual operations or transactions has been substantially strengthened and improved since the first evaluation round. Notifications now go to the UPB, not the courts, on the basis of simple suspicion. The number of notifications received (14 between July 2001 and February 2002) remains modest - but is at any rate far higher than under the 1995 Act. An administrative penalty was imposed on a bank by the CSF for failing to notify such a transaction, and one of its directors was temporarily suspended.

9. In Andorra, mutual legal aid in criminal matters is governed by the "Transitional Act on Judicial Procedure" (Section 52) and the first part of the Act on International Criminal Co-operation and the Fight against Laundering of Money or Assets derived from Organised Crime. Accession by Andorra to the European Convention on Mutual Assistance in Criminal Matters is now being considered. Interpretation of the requirement of dual criminal liability has not changed since the first cycle.

10. MONEYVAL also notes the clear desire of the authorities and sectors concerned to preserve the integrity and credibility of the Andorran financial market. Andorra is sufficiently aware that the integrity of the financial services market depends on the conviction that it operates in accordance with clearly-defined and stringent legal, professional and ethical standards. Although Andorra is a well-established financial centre and takes fairly comprehensive action to combat laundering, further action is needed to strengthen the prevention and control machinery and ensure that it is effectively deployed. Such action would cover such things as definition of offences, confiscation and provisional measures, ceilings for transactions and the use of cash, international co-operation, increased resources and greater independence for the institutions which supervise financial and other bodies subject to legal obligations, and – finally - training. Some of the professions specifically covered by the Act did not seem to take it sufficiently seriously at the time of the visit.

11. The 2000 Act is clearly geared to laundering of the proceeds of international crime and sets out, above all, to improve international co-operation – somewhat neglecting certain important aspects of domestic criminal law in the process. Moreover, it does not reflect some of the points made at the time of the last evaluation, which remain in abeyance. These are points which the first-round report considered particularly important - inter alia, in the light of recent international trends regarding supervision and verification of financial transactions. Specifically, the new Act does not prohibit cash transactions (€15,000), thus leaving considerable scope for the use of cash, which, moreover, does have to be declared to the Andorran Customs on leaving or entering the country. Nor are bankers and other financial operators required to record all cash transactions in excess of €15,000 in a special register. Banks may conduct exchange and currency operations freely, but are still not required to notify movements from/to other countries, which would make it possible to identify reasons for the transaction, destination countries, amounts and payees - although several European countries have long since adopted these recommendations.

12. MONEYVAL sees no notable changes in the structure of the financial sector. Andorra still has no public body with the powers normally vested in authorities responsible for monitoring financial systems. The economic and proprietorial status, and also the solvency of banks and other financial operators are still checked by external auditors, and the INAF still receives the reports and any recommendations made by these auditors, who may not inspect intermediaries, unless expressly authorised to do so by the CSF. To ensure effective supervision of the whole Andorran financial

[1] It joined the Egmont Group in 2002.

system, MONEYVAL considers that the INAF should, as a matter of priority, be given the independence and resources it needs to carry out inspections.

13. The Act on Commercial Companies still restricts foreign holdings in companies covered by Andorran law to 1/3 of their authorised capital. This limit may be exceeded in the case of public interest companies, for which the government determines the ceiling. During the visit, it became apparent that there were also de facto companies, whose establishment and dissolution were not covered by law. There are no civil-law professional partnerships. It was not clear, either, which profession advised on the establishment and winding-up of companies, since the representatives of the legal professions who talked to the evaluators denied doing this. The Trade Decree of October 1981 prohibits the use of borrowed names, although the Andorran authorities admitted that this practice still exists.

14. MONYVAL specifically recommends that consideration be given to a special law, which would retain the explicit prohibition on improper fiduciary activities (such as the use of borrowed names), but would allow a few specialised and supervised operators, such as banks and finance companies, to engage in transparent trustee-type operations (proper identification of clients).

15. Numbered accounts are still largely used, and certainly account for a substantial part of the business done by banks. These accounts are managed by staff specifically appointed for that purpose by banks, although the identification procedure is the same as for named accounts.

16. Andorra should also establish a consistent system for the registration of deeds covering property transfers such as a register of immovable property, centralised by a public authority and open to public inspection.

17. The new Act of 29 December 2000 makes no change in the list of offences connected with money-laundering, of which there are at present only 5: drugs-trafficking, illegal confinement, illegal arms-sales, procuring and terrorism; this obviously places some restrictions on international legal co-operation, and might even prove a barrier to such co-operation by the UPB. MONEYVAL takes good note of the work at present being done by the Parliamentary Commission of the Andorran General Council responsible for reviewing the Criminal Code, and hopes that the necessary changes, particularly regarding definition of the crime of money-laundering, will be adopted as soon as possible. The list of principal offences would then be dropped. There is, however, no plan to include tax-evasion among the principal offences.

18. The figures supplied by the Andorran authorities show that there has been only one final conviction for money-laundering since the start of the first evaluation round.2 The main obstacle to prosecution and conviction remains the need to prove that funds are unlawfully derived and, more particularly, derived from one of the five offences listed in the Criminal Code. The burden-of-proof requirements have in money-laundering cases have not changed since the first round. The excessive length of investigations, sometimes making it impossible to keep the persons concerned on remand, is also said to have hindered prosecution.

19. Legal entities may also be prosecuted for money-laundering, but no such cases had been brought in Andorra at the time of the visit.

20. In the criminal field, there have been no changes regarding provisional measures and confiscation since the first evaluation round. In the administrative field, however, the UPB has power to block a transaction for a maximum period of five days. After that, the transaction must be allowed to proceed, or the matter referred to the Public Prosecutor.

[2] However, there has been a second final conviction, upholding a sentence passed in 2001, since the visit in September 2002.

21. The report also contains recommendations and comments on various points which it brings to the Andorran authorities' attention, with a view to further strengthening of the country's anti-laundering system.

Cyprus

22. Cyprus was the 2nd PC-R-EV member State whose anti-money laundering regime was assessed in the framework of the second round of mutual evaluations conducted by Committee PC-R-EV. A team of PC-R-EV examiners, accompanied by colleagues from a Financial Action Task Force (FATF) member State and from the Offshore Group of Banking Supervisors (OGBS) visited Nicosia from 19 to 21 September 2001. The purpose of this evaluation visit was to take stock of the developments which occurred since the first round evaluation (i.e. April 1998) and to assess the overall effectiveness of the Cyprus anti-money laundering system in practice.

23. The crimes which are considered to be the major sources of illegal proceeds continue to be fraud, drug trafficking and smuggling offences (e.g. cigarettes). A limited number of organised crime groups are reported to be present in Cyprus and involved mainly in illegal drugs trafficking, extortion, prostitution and illegal gambling schemes. The Cypriot authorities emphasise the international character of money laundering, arising as a result of the country's development as an international business centre.

24. The methods of money laundering have not changed much since the first round. The banking sector is generally considered as the most vulnerable one to money laundering. Laundering operations may involve "international business companies" (IBCs) registered in Cyprus, which, formerly known as "offshore companies", have reached a record of 47,000 in 2001. Out of these, only about 1,080 entities maintain a physical presence in Cyprus in 2000.

25. The central piece of legislation in the Cyprus anti-money laundering regime is the Prevention and Suppression of Money Laundering Activities Law of 1996 (1996 Law), which has been amended several times since the first round evaluation. These amendments included the replacement of the former "list approach" by a new "all-crimes" provision stating that "predicate offences are considered to be all criminal offences punishable with imprisonment of more than one year, from which proceeds were derived".

26. Apart from the adoption of the "all-crime" approach, no change occurred in the definition of money laundering. 5 convictions have been obtained since the first round, mainly related to "own proceeds" laundering. These convictions were all domestic money laundering cases in which the predicate offences were fraud (obtaining money by false pretences) and drug trafficking. Significantly, none of them was based on a suspicious transaction report (STR), but on police investigations into predicate offences. The Cypriot authorities admitted that it was difficult to prove the connection between a suspicious transaction and extraterritorial predicate offences. However, there are 11 cases pending before courts and at least one of them is related to a "classic" and also sophisticated money laundering activity (involving various bank transactions).

27. There have been no changes with regard to the comprehensive and robust system of provisional measures. The statistics concerning the application of provisional measures and confiscation in practice show that provisional measures, such as freezing and restraint orders, are applied more and more frequently. However, the examiners recommended that these powers should be used by MOKAS from the earliest moment of their intelligence work and that MOKAS should formally be empowered to suspend financial transactions.

28. Confiscation is conviction based and can be ordered in relation to criminal proceeds or the corresponding value. Given the low number of confiscation orders compared to the restraint and freezing orders, the examiners think that much remains to be done in this area.

29. A very positive feature of the regime is that legal entities can be held liable for money laundering and criminal offences generally. It would however seem that there have so far been no instances in which legal persons were effectively prosecuted under the provisions of the 1996 Law. Therefore, the examiners recommended that the Cypriot authorities carefully examine why money laundering prosecutions did not involve legal persons.

30. Institutionally, the anti-money laundering regime Cyprus rests on two key institutions: the Unit for Combating Money Laundering (MOKAS), the Cypriot FIU, and the Central Bank of Cyprus (CBC), the main regulator and supervisor in the financial sector. Following the recommendations made in the first round evaluation report, MOKAS has already been strengthened. However, given its multiple functions, the examiners think that MOKAS is still understaffed and recommend its further reinforcement, in terms of personnel (more financial analysts), IT facilities and financial resources. In addition, specialisation of staff and restructuring are highly recommended at MOKAS.

31. The Cyprus Government has also appointed new supervisory bodies under the 1996 Law for lawyers and accountants. Though this is welcomed by the examiners, they consider that neither of the two bodies is equipped to undertake this responsibility as self-regulatory bodies. They recommend that this responsibility is transferred to or shared with MOKAS or the CBC so as to ensure effective monitoring of compliance by these professions with their anti-money laundering obligations.

32. There has been much progress achieved in the financial sector since the first round evaluation, through more awareness in the sector, the issue of guidance notes by the different regulators and, to an extent, by the formation of associations for different sectors of the financial market, even if there might to be too much reliance in laying responsibilities on the CBC. The examiners particularly welcome the active role played by the CBC with respect to guidance: the CBC issued a number of new guidance since the first round, e.g. prohibiting the acceptance of cash deposits in foreign currencies in excess of US$ 100.000 without the prior written approval of the CBC, requiring banks to refer to the CBC for guidance applications that they receive for the opening of accounts in the name of "banks" incorporated in specified offshore jurisdictions, requiring banks to verify the identity of corporate customers by obtaining a series of documents and to take appropriate measures to establish the identity of persons, both physical and corporate, on whose behalf trustees and nominees are acting, etc.

33. However, the examiners consider that the high number of regulators for the size of the Cypriot market has resulted in a shortage of adequate and sufficient staff, which curtails expertise in the regulatory function of the different regulators. On the other hand, the area of domestic investment services and advice is still not regulated.

34. Trustee and nominee services in Cyprus are provided by International Trustee Companies, lawyers and accountants. At the time of the on-site visit, the possibility existed for banks to disregard their obligation of identification and rely, when opening an account the beneficiary of which has not been identified on identification carried out by regulated trustees and nominees, acting as business introducers. The examiners recommend to change this practice.

35. MOKAS, as an FIU, needs financial intelligence to perform its functions (e.g. when analysing suspicious transaction reports (STRs)) and for that purpose information held by other regulatory bodies needs to be shared with it, including aggregate information on cash-transactions and other data held by the CBC, which may be useful for MOKAS' financial intelligence work. The examiners noted in this regard that banks should not hold preliminary discussions with the CBC to establish whether or not an STR has to be filed with MOKAS.

36. Since the first round MOKAS has received an ever increasing number of (STRs) filed by institutions or persons obliged to report. The large majority of this increase had in fact come from the banking sector. Therefore, further efforts need to be done to make the reporting system more balanced.

Moreover, MOKAS should monitor the spread of reporting and periodically examine for example how many of the onshore banks and offshore banks are filing STRs and how these figures compare.

37. In the area of international co-operation, there is an obvious willingness of the authorities to co-operate with overseas jurisdictions. No problems were indicated to the evaluation team in this area, neither in responding to informal requests nor in the execution of subsequent formal rogatory letters.

38. Overall, Cyprus has made since the first round further progress towards building an effective and robust anti-money laundering regime. With the exception of the legal professions, there is a strong commitment from all institutions in the system, including the private sector, to join the anti-laundering effort. Cyprus has also reacted positively to most of the recommendations made in the first round evaluation report and its legal framework starts producing results. However, a certain number of issues remain, in particular with regard to the resources dedicated to MOKAS and the supervision of insurance sector.

Czech Republic

1. A PC-R-EV team of examiners, accompanied by a colleague from the Financial Action Task Force (FATF) visited the Czech Republic between 8-11 October 2001. This visit took place in the framework of the second round evaluation. Its aim was to take stock of developments since the first round evaluation (i.e. May 1998 in the case of the Czech Republic), and to assess the effectiveness of the anti-money laundering system in practice.

2. There have been no significant changes in the types of criminal activities considered to be the major sources of illegal proceeds. However, the criminal activity in the economic field has become increasingly sophisticated and specialised, some banks being at the same time infiltrated by criminals. The latter take advantage of the developed financial infrastructure including the securities market and the unlimited use of cash payments. Limits on cash transactions are not envisaged by the Czech authorities for the time being. On the other hand, new bearer passbooks cannot be issued and the examiners were advised that from 1st January 2003, only total withdrawal will be allowed and this will be subject to identification requirement.

3. The government strategy on combating organised crime of 1997 was assessed and updated accordingly in October 2000. Targeting the revenues of crime are an element of this renewed strategy. Recognising the importance of having an effective anti-money laundering regime, the Czech government also approved in April 2000 a written document analysing the effectiveness of the domestic anti-money laundering regime. This document requires the adoption / implementation of a number of measures considered crucial to better address money laundering issues (reversal of the burden of proof, confiscation, limitation of cash transactions, central files of account holders, specialisation of the police etc.). The government accordingly introduced legal amendments, on the basis of recommendations from the EU (the Czech Republic applied for EU membership) and from the PC-R-EV first evaluation round, but also based on the national experience deriving from the implementation of existing legislation. One important element of the recent changes was the amendment of Act No. 61/1996 (the Anti-Money Laundering Act), effective on 1st August 2000. Furthermore, the government enacted a so-called "Euroamendment" to the Criminal Code which comprises a new body of crime of the criminal offence of legalisation of proceeds from criminal activity (Section 252 a). This new amendment will enter into force on 1st July 2002. Other recently decided amendments include those to the Criminal Procedure Code and to regulations related to the economic environment of the Czech Republic.

4. The capacity of the Czech Republic to cooperate internationally was further enhanced with additional bilateral agreements between the FAU and foreign counterparts, and with assets-sharing agreements with the US and Canada. All international conventions ratified by the Czech Republic are directly applicable in the country.

5. The basic provisions criminalizing money laundering at the time of the visit are the same as those in force during the first round evaluation (Sections 251, 251a and 252). Their weaknesses therefore remain (e.g. inconsistency with the definition of laundering provided by Act 61/1996; self laundering is not covered; the concept of "thing" is too narrow and too far from the Strasbourg Convention definition of proceeds and property). The new provisions of Sections 252 and 252a expected in July 2002 would bring some improvements on the previous position: laundering of "own proceeds" would appear now to be covered with the deletion of the words "enables another person" from Section 251a; the concept of "thing" in Section 252a would be supplemented with less tangible products of crime ; the penalty for negligent money laundering would be increased. It remained unclear to the evaluation team why the Czech authorities have not spelled out in the Euroamendment clearly that the Czech Republic can exercise jurisdiction in a money laundering case where the predicate offence is committed abroad. The physical elements of the offence remain based on the concealment. It remains debatable whether the "acquisition, possession or use" of laundered proceeds really are covered in the new money laundering legislation. Likewise, the mental element in Sections 252 and 252a has not been revisited. Presumably the full rigours of knowledge standard remain. The two offences seem to be either intentional or negligent.

6. Finally, the statistics available show few prosecutions under the Section 251a - which, in any event, appears not just to cover money laundering. A fresh criminal offence, based clearly on the terms of the Strasbourg convention and clarifying all previous ambiguities would be far more helpful for the fight against money laundering. Additional practical measures, such as guidelines, would help the police, prosecution and judges to make a better use of the existing provisions.

7. This second round evaluation confirmed both in theory and practice that confiscation is still an alternative to punishment rather than a systematic measure targeting the proceeds of crime. As a matter of fact, the application of confiscating measures is left to the court's discretion and figures concerning the frequency of confiscation and the amounts concerned are not available. On the other hand, the recent creation of a Proceeds from Crime Department within the police, and the first positive results obtained by this Department in terms of seizures are encouraging. The prosecutors and the judges need to be as committed to this agenda as the new department. There needs to be a concerted and agreed approach to the importance of the confiscation agenda by police, prosecutors and judges backed up by an enabling legal regime which will ensure significant disruptive confiscation orders of the direct and indirect proceeds of crime.

8. The Law 61/1996 was amended and the preventive regime against the use of the financial sector for money laundering was improved to a large extent (e.g. the concept of "suspicious transactions" was introduced; move from "contact persons" to "money laundering compliance officers, extension of the record keeping requirement to documentation on transactions, requirement to identify "third persons", rules on professional secrecy etc.). Clear anti-money laundering responsibilities and supervisory powers were granted to the Czech National Bank, the Securities Commission, and the Cooperative Savings Unions regulatory bodies. The means of the FAU were enhanced, and training was developed. The current system could be further improved with the introduction of a clear requirement to identify beneficial owners and with a better and more systematic feedback from the FAU to reporting entities. The supervision over the financial sector could also be strengthened in various ways : rigorous on- and off-site controls, sanctions in case of non-observance of the requirements etc. Some sectors considered as vulnerable should be subject to closer attention.

9. As regards the FAU, the recent recruitment of additional analysts has increased its working capacity in this field. The computerisation of work was improved too with adequate software made available and the FAU has now access to the main relevant databases (including those of the police, tax administration and Customs). All this was needed if one considers the rather modest performance of the FAU in recent years. Out of 956, 1699 and 1920 STRs received in 1998, 1999 and 2000 respectively, only a – comparatively - limited number of complaints were lodged (37 in 1998, 47 in 1999 and 103 in 2000). International cooperation and collaboration with the financial sector is considered satisfactory. The FAU is also actively involved in provide training and raising awareness of

the private sector and other authorities' staff. The evaluation team was concerned about the staffing of the FAU's Legal and Inspection Department: its four staff are insufficient to carry out all on- and off-site controls falling within its jurisdiction in the Czech Republic. Consequently, the staffing of the Department needs to be reconsidered. For the time being, the FAU does still not consider using liaison law enforcement personnel to assist it in the operational field.

10. Despite the recent creation of specialised prosecution sections and greater specialisation of the police to deal with economic crime cases including money laundering (see also above, the Proceeds from Crime Department), the work of the prosecution and police remains difficult in these fields. Various secrecy provisions and limits on the use of special investigative techniques undermine the overall investigative capacities. At the same time, there is a need for more targeted training in economic crimes and money laundering. All these factors are likely to make the repressive authorities prefer to initiate fraud-related cases, instead of money laundering cases, and to prefer focusing on the predicate offence. As a consequence, there has been no money laundering case since the first round evaluation. These problems need to be addressed.

11. The Czech Republic has adopted a number of measures since the first round evaluation. By addressing the issues above, the Czech Republic can improve the fight against money laundering and make the regime to combat it more effective

Hungary

1. Hungary was the sixth Moneyval member State whose anti-money laundering regime was assessed in the framework of the second round of mutual evaluations conducted by the Committee. A team of Moneyval examiners, accompanied by two colleagues from Financial Action Task Force (FATF) member States visited Hungary from 3 to 6 December 2001. The purpose of this evaluation visit was to take stock of the developments which occurred since Hungary's the first round evaluation (i.e. October 1998) and to assess the overall effectiveness of its anti-money laundering system in practice.

2. The money laundering situation has not changed significantly since the first round evaluation. Economic crimes, tax fraud, smuggling, crimes against property, such as theft, robbery and fraud, continue to be considered the main sources of illegal assets. Drug trafficking, prostitution and extortion are also potential sources of criminal proceeds. Organised crime is believed to be involved in committing both predicate crimes and laundering operations.

3. The methods of money laundering have not changed much either since the first round: in the placement stage, laundering operations usually involve cash exchanged and deposited in financial institutions followed by the misuse of bank accounts for subsequent wire-transfers. Offshore or fictitious companies play a significant role in the layering stage of these operations, e.g. to justify wire-transfers. In the integration phase, proceeds are often re-invested in companies, including offshore companies, active in the catering and service sectors. The purchase of real estate, bearer securities and stocks also provides opportunities for laundering cash proceeds.

4. Given its crime situation and reacting to international requirements, Hungary has significantly improved its anti-money laundering regime since the first round. These changes reflect a new attitude of the Hungarian Government, which regards the fight against money laundering and the financing of terrorism as a priority issue on its agenda. It is recalled that the first evaluation report raised many issues of concern and included a number of recommendations for the improvement of Hungary's anti-money laundering (AML) system, in relation to the legal framework, measures in the financial sector, as well as on the operational level. In addition, Hungary was listed by the FATF among the "Non Co-operative Countries and Territories (NCCT)", between June 2001 and June 2002. To address such criticism and to increase the overall effectiveness of its anti-laundering regime, the Hungarian authorities, inter alia :

- Introduced new legislation effective from 19 December 2001 to extend the scope of the 1994 AML legislation to a large number of professions outside the financial sector in line with the relevant European Union Directives, explicitly obliged financial intermediaries subject to the AML legislation to identify the beneficiary owner in all transactions and subjected currency exchange services to stricter licensing and operational conditions and procedures;
- Amended in March 1999 criminal law provisions related to the money laundering offence (section 303 of the Criminal Code) by introducing the "all crimes" approach for predicate offences and to the confiscation of assets, which became mandatory for all offences in the course of or in relation to which assets were obtained.
- Improved financial supervision by setting up from 1 April 2000 a new single supervisory agency, the Hungarian Financial Supervisory Authority (HFSA), which was tasked to supervise banking and credit institutions, insurance companies and other financial institutions, including their active anti-money laundering supervision;
- Created a high-level policy-making and co-ordination body, headed by a special government Commissioner, to co-ordinate the different authorities and institutions involved in Hungary's anti-money laundering system;
- Abolished bearer (savings-deposit) passbooks, including the prohibition to open new passbooks and the phasing out of existing ones in a graduated procedure. Accordingly, credit institutions may only accept savings deposits from clients duly identified and registered. Equally, only registered securities can be offered to the public or issued in series;
- Regulated foreign exchange services so that from 1 January 2002 only credit institutions and their agents may be authorised by the Hungarian Financial Supervisory Authority (HFSA) to offer currency exchange services. Under the new regulations, managers and employees of bureaux de change will be subject to enhanced scrutiny, including verification of their criminal records;
- Strengthened the FIU, whose staff was significantly increased ;
- Intensified the training provided for the staff of financial service providing organisations.

5. With these changes, the examiners consider that all serious shortcomings previously identified have been corrected and that most if not all recommendations made in the first round report were positively responded to. They also note with satisfaction that since the on-site visit, several additional measures were introduced in the area of prevention and criminal law. Hence, the examiners consider that Hungary is generally in compliance with the requirements embodied in the 25 other (NCCT) criteria.

6. However, this new AML regime, which has become robust and comprehensive, needs to be firmly rooted in domestic practice. In addition, the examiners of the second round evaluation have identified some issues which need further addressing in the system and made recommendations for improvement. These issues are primarily related to the implementation of the AML legislation and the lack of results in the criminal justice area.

7. In the area of prevention, the compliance level in general is satisfactory, but certain professions need further attention. The Hungarian authorities need to ensure that the legal professions subject to the expanded 1994 AML legislation are provided with guidance as soon as possible, so as to enable them to prepare internal rules and thus help compliance control. This is particularly urgent for those professions which have no experience in implementing AML measures or still resist their new responsibilities. Further training of these professions is also a key to their effective implementation of the AML - regime. A particular area where guidance is urgently needed - across the financial sector - is the identification of the beneficial owner.

8. The reporting of suspicious transactions has improved in quality and increased in number since the first round. The Hungarian FIU has received over 3000 STRs during this period. However, the number of criminal investigations based on the STR-system is still rather modest. This lack of

effectiveness should be closely monitored by the Hungarian authorities. In this context, the examiners detected a potential risk of over-reporting by certain banks, which might stem from the current level of liability on employees or an erroneous interpretation of the role of the compliance officer. Moreover, they noted that in Hungary's AML-regime the power to suspend suspicious transactions has been "delegated" to the financial service providers. This creates vulnerabilities with regard to liability challenges and financial damages, which many other jurisdictions have addressed by placing the power to suspend transactions with the FIU.

9. Despite highly motivated police staff, criminal investigations into money laundering are seldom successful and indicate insufficient co-ordination and/or focus on criminal assets. The examiners consider that law enforcement results need to improve in general and that further training in financial investigations and a higher level of co-ordination within the police may bring improvement in this area.

10. The legal framework in the area of criminal law is generally sound but clearly should generate more confiscations and convictions. Hungary's criminal justice system so far obtained only 1 conviction, which the examiners believe is partly due to diverging interpretations as to the proof requirements of the money laundering offence. They recommend that the Hungarian prosecution authorities give unambiguous instructions to prosecutors on the interpretation of the money laundering offence and the related evidentiary requirements, or amend the definition of money laundering, as appropriate.

11. Equally, the amount of criminal assets recovered from criminals is not commensurate to the considerable efforts made by the Hungarian authorities. The examiners believe that further substantial efforts are necessary to retrieve and recover criminal assets. This particularly applies to the criminal justice authorities during the whole process from police investigations through prosecutions to court cases.

12. In the area of international cooperation, much progress has been made, but the examiners recommend the review of the provisions regarding the implementation of foreign orders for provisional measures or confiscation as well as the adoption of regulations on the sharing of confiscated assets. They also advise that the Hungarian authorities proceed with the necessary arrangements to keep records and statistics on mutual legal assistance requests (including freezing and confiscation orders).

13. As commercial - often front - companies seem to play a increasingly important role in money laundering operations in Hungary, the examiners noted with concern that the current system of company registration does not allow the routine identification of beneficial owners, in particular foreign ones. In addition, Hungary offers offshore corporate services, i.e. the registration and operation of international business companies (IBCs), of which approximately 600 exist at present but will need to be abolished by 2005. Their activities cannot be easily monitored and the examiners believe that the current registration process is too easy and may be misused. Pending the phasing out of these companies, they recommend that the Hungarian authorities urgently take the necessary arrangements in order to develop a registry of the beneficial owners of these companies, which will be accessible to the FIU and other law enforcement authorities. They further recommend that the Hungarian Courts of Registration be required by law to obtain the identity of the real owners (including natural persons as ultimate beneficial owners) before the registration of a company.

14. The evaluation team believes that the adjustments proposed would contribute to making Hungary's anti-laundering regime produce more results and thus become a fully effective system.

Malta

1. Malta was the 7th Moneyval (PC-R-EV) member State whose anti-money laundering regime was assessed in the framework of the second round of mutual evaluations conducted by the

Committee. A team of four examiners, including a colleague from a Financial Action Task Force (FATF) member State, visited Valetta from 14 to 17 January 2002. The purpose of this evaluation visit was to take stock of developments that occurred since the first round evaluation (in September 1998) and to assess the overall effectiveness of the Maltese anti-money laundering system in practice.

2. In general, Malta's crime situation has not changed since the first round, though in recent years illegal immigration and trafficking in human beings have increased among profit-generating activities. There are no locally based organised crime groups in Malta, but Maltese citizens and companies registered in Malta may be involved in the activities of international criminal groups, including money laundering operations. Fraud and drug trafficking are still considered as the main sources of illegal proceeds.

3. While money laundering is still a potential threat, the overall risk for Malta has reduced with the process of phasing out the offshore sector by September 2004 and the reform of the nominee regime. Nevertheless, exposure to risk still remains in the financial sector, considered as the most vulnerable to money laundering, but laundering operations could possibly involve the real estate sector, companies and financial services providers as well.

4. The central piece of legislation in the Maltese anti-money laundering regime is the Prevention of Money Laundering Act, 1994 (PMLA 1994), which has been amended several times since the first round evaluation, including in December 2001 by the Prevention of Money Laundering (Amendment) Act, No. XXXI of 2001 for the purpose of setting up the Financial Intelligence Analysis Unit (FIAU). The PMLA 1994 is supplemented by the Prevention of Money Laundering Regulations, 1994 (PMLR 1994), which sets forth the preventive obligations under the Maltese anti-money laundering regime, and legally binding Guidance Notes. These elements constitute together a comprehensive and robust legal framework, which is commended by the examiners.

5. On the criminal law side, money laundering is still criminalised by a number of laws: while the PMLA 1994 criminalises money laundering offences in general, based on a wide list of predicate offences, two earlier ordinances (Dangerous Drugs Ordinance, 1939 and Medical and Kindred Professions Ordinance, 1901) criminalise drug-related money laundering. The list of predicate offences under the PMLA 1994 was further expanded in 1999 to include any serious crimes, though these do not cover tax offences. Negligent money laundering has not been criminalised. While this broader list of predicate offences under the PMLA 1994 is welcome, the examiners recommended that Malta consider harmonising drug and non-drug money laundering offences as well as changing the general definition currently based on a list of predicate offences to an "all-crime" one.

6. During the period of 1998 – 2001, the Maltese authorities have initiated 6 prosecutions for money laundering, none of which resulted - at the time of the second round visit - in convictions. In this regard, the examiners expressed concern about the potential impact of a preliminary judicial decision, handed down in November 1999 by the Court of Criminal Appeal and quashing the by then only indictment for money laundering for lack of evidence. Bearing in mind that the number of money laundering investigations during this period was over 100, the examiners felt that the criminal justice system was not producing the expected results, despite the high-quality of the legal framework. This was believed to be partly due to the Court's interpretation of evidentiary requirements for prosecutions to succeed, which the examiners recommended for further consideration, possibly through the Prevention of Money Laundering Joint Committee. They also recommended training for all criminal justice personnel on money laundering-related issues and that prosecutors should seek to impress upon judges the autonomous nature of money laundering as well as the need to draw the necessary inferences from the evidence produced.

7. Controlled delivery and purchase of drugs are provided for under the ordinances and require the prior consent of either the Attorney General's Office or a magistrate. These techniques can be used by the Police in money laundering investigations, but all other types of special investigative powers, such as telephone interception or other surveillance activities, can only be carried out by the Security

Services for the Police. A wider use of special investigative techniques by the Police was therefore recommended in order to improve the rate of successful money laundering investigations, and the authorities were also invited to consider how to improve the use of information gathered through the use of such techniques in judicial proceedings. The evaluation team welcomed the setting up of a special unit within the Police to deal with money laundering investigations, in particular as it noted serious difficulties in gathering the necessary evidence for money laundering investigations and a backlog of cases pending or finished without prosecution. It further noted that this situation was expected to change with the setting up of the Financial Intelligence Analysis Unit (FIAU), which since 2002 has taken over from the Police the STR-related intelligence work. The evaluation team has also recommended a more asset-oriented approach in law enforcement, e.g. in relation to financial crime.

8. At the time of the second round visit, there was no change in the legal regime of provisional measures and confiscation but the results of the current regime were found to be rather disappointing: while the number of investigations ordered in money laundering cases, including those based upon international cooperation, has been systematically growing since 1998, no similar tendencies could be observed as to the provisional measures taken. Even if considering the size of Malta, such measures do not seem to be applied frequently enough and neither could any remarkable development be observed in terms of the amount of the property seized or frozen. In addition, as the Maltese confiscation system is conviction-based, there were no confiscations obtained in relation to money laundering cases. Therefore, the examiners welcomed that at the time of the second round visit, Malta was already in the process of amending its Criminal Code that would also bring changes in this field, e.g. through the extension of freezing and forfeiture orders to all offences punishable by imprisonment of at least one year and the amendment of the PMLA 1994 providing for the shifting of the burden of proof on to the accused with respect to proof of the lawful origin of proceeds in the absence of a reasonable explanation by the accused, in relation also to offences of money laundering under the said Act, and providing for the forfeiture of proceeds from legal persons.

9. With regard to corporate liability, the examiners noted with satisfaction that the Maltese authorities were in the process of amending the Criminal Code to introduce a specific provision enabling the application of criminal penalties (fines up to 500,000 Liri) to corporate entities in relation to serious crimes, and that a similar provision would be made to the PMLA 1994 concerning money laundering.

10. For enhancing international cooperation, Malta has signed a number of bilateral agreements and ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (the "Strasbourg Convention") on 19 November 1999, which came into force in March 2000. In this context, the examiners recommended that the Maltese authorities keep under review the reservations made to this Convention and consider the possibility of revoking them. In general, the examiners noted the positive and helpful attitude of the Maltese authorities in international cooperation, which during the review period involved 22 rogatory letters sent to Malta – all of which have been answered – and the sending of 1 request by Malta. The examiners pointed out the potential limiting effect on international cooperation of Malta's list-based money laundering offence, but noted that that even in cases related to fiscal offences, assistance could be provided under certain circumstances, though this assistance would not enable the application of coercive measures.

11. On the preventive side, several important changes occurred since the first round, such as the abolition of bearer accounts from 30 June 2000 by decision of the Central Bank of Malta and the issue of a directive by the latter and identical directives by the Malta Stock Exchange (MSE) and the Malta Financial Service Centre (MFSC) in March 2001 for all banks, stockbrokers and other investment and financial institutions to refrain from undertaking transactions in which nominee shareholding is involved unless they obtain the full disclosure of the beneficial owners. Malta also continued the phasing out of its offshore sector, in accordance with the decision taken in 1994 to close down this sector by 2004. At the time of the visit, around 300 offshore companies remained of the 2600 that had existed.

12. The examiners also noted that the sectoral Guidance Notes issued by the various regulators under statutory authorisation will be amalgamated into a single comprehensive set, but have not been issued at the time of second round on-site visit.

13. The examiners also welcomed the setting up of a single financial regulator, the Malta Financial Services Authority (MFSA), which will license and supervise all activities related to financial services (banking, insurance, investment services and securities) in Malta, while the supervision of compliance with the anti-money laundering legislation will be vested with the new Financial Intelligence Analysis Unit (FIAU), also set up in 2002. The range of regulated entities has not changed since the first round: the PMLR 1994 still cover business related to banking, financial, life assurance, investment and stockbroking activities, casinos, and under certain conditions, auditors, lawyers, notaries and accountants, who are in general not considered as subject persons.

14. The examiners noted with satisfaction that in general, since the first round, money laundering has been an area of attention for all supervisors. This was in particular visible in the insurance sector, which was previously criticised for poor supervision. It was however noted that certain sectors still needed further attention, such as investment services and the securities market, despite recent efforts by the MFSC to enhance supervision in these areas.

15. In the financial sector, compliance with the PMLR 1994 has been in general found satisfactory, but vigilance was recommended with regard to non face-to-face transactions. The examiners also recommended further clarification in the Guidance Notes for the current customer identification procedures under Regulation 5 so that financial institutions understand better that they have to obtain satisfactory evidence of the prospective customer's identity always prior to establishing a business relationship or conducting a transaction.

16. The examiners noted that the management of the company Registry was transferred to the MFSA, which was not expressly required to control the authenticity of the information submitted to it.

17. As far as the reporting of STRs is concerned, the examiners noted that while there was a modest increase since 1999 (1999: 19; 2000: 28; 2001: 31), the bulk of the STRs was still filed by onshore banks (1999: 68.4%; 2000: 82.1%; 2001: 67.7%), that no STRs were filed by insurance companies or other non-bank financial institutions. The examiners recommended an increased supervisory vigilance when inspecting supervised entities as to the observance of their reporting obligations, including the documentation on any non-reported case, and that the FIAU keep the under-reporting sectors under close scrutiny and apply the appropriate measures to trigger better reporting behaviour if necessary.

18. In general, the examiners concluded that Malta had made substantial progress since the first round in consolidating its legal framework and preventive regime against money laundering. Though some of these reforms have not yet been fully implemented in practice at the time of the on-site visit, the evaluation team welcomed the commitment of the Maltese Government to continuously upgrade and perfect the overall anti-money laundering regime. Malta now has a robust criminal legislation in place and a particularly well-regulated financial sector. However, certain sectors still need to be brought under the remit of the PMLR 1994 and the new supervisory arrangements have to prove their efficiency in practice. The results of the criminal enforcement at the current stage are disappointing, both in terms of money laundering convictions and confiscations. The police and the judiciary particularly need training to understand the challenges posed by money laundering investigations and prosecutions. With the rapid implementation of the recommendations in this report, the evaluation team believes that Malta will be able to improve the results soon.

Slovenia

1. Slovenia was the first PC-R-EV member State whose anti-money laundering regime was assessed in the framework of the second round of mutual evaluations conducted by Committee PC-R-EV. A team of PC-R-EV examiners, accompanied by a colleague from a Financial Action Task Force

(FATF) member State visited Slovenia from 9 to 12 July 2001. The purpose of this evaluation visit was to take stock of the developments which occurred since Slovenia's the first round evaluation (i.e. April 1998) and to assess the overall effectiveness of its anti-money laundering system in practice.

2. The money laundering situation has not changed significantly since the first round evaluation. Drug trafficking is still considered to be the main source of illegal proceeds. In the period under review, the number of detected drug trafficking offences continued to grow. Other important sources of illegal proceeds are fraud, trafficking in weapons, illegal immigration, currency and securities counterfeiting as well as extraterritorial offences such as tax evasion, tax fraud (especially VAT fraud), corruption and abuse of office. Organised crime is believed to be involved in both predicate crimes (e.g. drug and weapon trafficking, illegal immigration and counterfeiting currency and securities) and laundering operations.

3. The methods of money laundering have not changed much either since the first round: they usually involve the misuse of non-resident accounts by non-residents from the neighbouring countries and from the countries of the former Soviet Union. Most of these accounts are opened on behalf of companies registered in off-shore countries Money launderers still use the Western Union money-transfer system in connection with the proceeds of illegal immigration.

4. Aware of this crime situation, the Government of Slovenia has been implementing since 1997 a special strategy for the prevention and detection of economic crimes. This strategy, which involves all Government agencies and in particular the Ministry of the Interior, aims at the prevention of economic crime through detection, crime analysis and standardised investigation measures, special training of law enforcement personnel and enhanced co-operation with other agencies, including co-operation with foreign law enforcement bodies. On 1 April 2000 a dedicated Economic Crime Section was created under the General Police Directorate, within the Criminal Investigation Police. This section includes the Financial Crime Division which is in charge of conducting preliminary investigation into money laundering cases as well as into other economic crimes.

5. As drug trafficking is considered to be the main source of laundered proceeds a joint Police and Customs group has been set up to deal with drug trafficking. In addition, specialised anti-corruption units were established at central and regional levels.

6. As far as prosecutorial bodies are concerned, the Law on State Prosecution was modified with effect from 8 July 1999 and the competences of the Group of State Prosecutors for Special Matters, set up in 1996 specifically for the prosecution of organised crime cases, including money laundering, were enlarged.

7. The quality of the preventive system based on the Law on the Prevention of Money Laundering (LPML) of 1994, has already been recognised by the first round evaluation report. At the time of the visit, a new anti-money laundering law was in preparation, which entered into force on 25 October 2001.

8. The Office for Money Laundering Prevention (OMLP), i.e. Slovenia's Financial Intelligence Unit, is at the very heart of the anti-laundering system. Though its financial and human resources have recently been increased, OMLP stills needs strengthening, particularly since the new anti-money laundering legislation is expected to further increase its workload with the proposed extension of the reporting duty to other professions.

9. During the period of 1998 – 2001 the OMLP has received 265 cases on suspicious transactions and between 1999 – 2000 72689 disclosures about cash transactions in excess of SIT 4,6 million. Though the reporting threshold for cash transactions has recently been increased from SIT 3,6 million to SIT 4,6 million, a further increase is envisaged to SIT 5 million.

10. Financial supervision, which was identified in the first round evaluation as one of the weak points of the system, has also been addressed but there is still room for improvement. The supervisory bodies (Bank of Slovenia, Securities Market Agency, Insurance Supervisory Agency, Office for Gaming Supervision) are more aware of their supervisory responsibilities and of the necessity to take their guidance role seriously. But the phenomenon of over-reliance on the OMLP is still perceptible, both legally and practically. The supervisory authorities of banks, non-banking financial institutions and those non-financial businesses which are subject to supervision (i.e. casinos) are not explicitly entrusted by the LPML with any supervisory powers or responsibilities. In particular, the control of the "fit and proper" condition of owners and managers of exchange houses is not up to the required standard, and that the monitoring and supervision of the latter as well as other non-banking financial institutions is still quite unsatisfactory.

11. The existence of bearer passbooks in Slovenia remains an issue which the examiners recommend to address urgently. Notwithstanding the identification of the client on opening the underlying account, no identification is made of the passbook holder concerning transactions below the threshold identification limit of SIT 2.8 million. Since bearer passbooks are transferable from one person to another, these passbooks effectively operate as anonymous accounts and as such are contrary to the spirit of FATF Recommendations and raise issues of compatibility with Recommendation 10. The Slovenian authorities are recommended to take measures to prohibit the operation of such accounts and the conversion of existing ones into normal passbooks where the usual customer identification requirements will apply.

12. The possibilities of international co-operation have continued to expand thanks to the multilateral and bilateral instruments to which Slovenia is a Party. Yet, this ever increasing co-operation may prove difficult to cope with given the limited human resources currently available at the Ministry of Justice. The examiners therefore recommend to strengthen the relevant division of the Ministry with additional staff as a matter of urgency.

13. Apart from police and FIU-related agreements, since the first evaluation Slovenia signed and ratified the European Convention on Mutual Assistance in Criminal Matters and its additional protocol of 1978. It also ratified the Council of Europe Criminal Law Convention on Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Moreover, Slovenia signed the Pre-Accession Pact on Organised Crime between the Member States of the European Union and the Applicant Countries and initiated the agreement on co-operation with Europol. Slovenia also signed, but has not yet ratified, the UN Convention on Transnational Organized Crime.

14. The Slovenian authorities have also made serious efforts to close certain legal gaps identified in the first round report, e.g. by the introduction of corporate liability under the new Law on the Liability of Legal Persons for Criminal Offences (which came into force on 23 October 1999), by regulating the possibility to confiscate criminal proceeds in the absence of a formal conviction (such as with the demise or disappearance of suspect - Art. 498 and 498a Code of Criminal Procedure) and by resolving the controversy on "self-laundering" with an express reference in Article 252 (2) Penal Code.

15. Given the high standard of the legal framework surrounding the anti-money laundering regime, the performance of the preventive system, the efficiency of the FIU and the commitment of the police, it is greatly disappointing to see that the system does not produce the results it deserves in terms of convictions and confiscation. All efforts in the anti-money laundering chain are being jeopardised by the judicial follow-up. The crucial problem would seem to be the nature and degree of proof required to prove the offence of money laundering and in particular the insistence on proof of the specific predicate offence postulated by the prosecution. There also seems to be substantial reluctance on the part of the judicial authorities to draw the pertinent inferences from circumstantial evidence which is very often the only available evidence in money laundering prosecutions.

16. The entire problem is compounded by the apparent over-cautious approach of the prosecuting authorities to take cases before the courts. Increased prosecutions would enable the courts to familiarise themselves better with the nature of money laundering and the operating methods of launderers and this could, in turn, encourage the courts to more readily draw the legitimate inferences from the evidence produced and which could result in increased convictions and confiscations.

17. This second round evaluation has also shown that the law enforcement effort is still predominantly crime-oriented. A more asset-oriented approach, in particular in relation to financial and fiscal crime is likely to contribute to the reversal of the current law enforcement approach. In relation to this, the creation of a police force to deal specifically with asset recovery and confiscation matters would be of value.

18. Overall, Slovenia has adopted a number of positive measures since the first round evaluation to further enhance the efficacy of its anti-laundering system. The examiners welcome these measures. However, some issues remain, which need to be addressed.

Slovakia

1. Slovakia was the 4th MONEYVAL (PC-R-EV) member state to be evaluated in the framework of the second round of mutual evaluations conducted by the Committee. A team of examiners accompanied by a colleague from a Financial Action Task Force (FATF) country visited Bratislava between 15-18 October 2001. The purpose of the evaluation was to take stock of developments which had occurred since the first round evaluation (in June 1998) and to assess the overall effectiveness of the Slovakian anti-money laundering system in practice.

2. Economic crime and fraud offences remain significant. Drug trafficking is a continuing problem, as is corruption and smuggling. These offences together generate the most criminal proceeds. Organised crime continues to be a major threat and it is known to be involved in money laundering operations and responsible for numerous categories of predicate offence, particularly drug trafficking.

3. Cash transactions are still an important feature of the Slovak economy, and as such money laundering continues to be a threat in the banking sector. The Slovak authorities are also conscious that money launderers may diversify into purchase of real estate, the purchase of precious stones and securities investment.

4. At the time of the on-site visit, the central piece of preventive legislation in place was Act 367/2000 (on protection against the legislation of incomes from illegal activities and on amendments of some acts). This Act came into force on 1 January 2001 and 9 months before the on-site visit. It replaced the previous anti-money laundering law (Act 249/94), which had a number of deficiencies, enumerated in the first evaluation report. In particular, that evaluation had highlighted that the sole reporting duty was on banks and there were no provisions for sanctions in respect of breaches of anti-money laundering legislation. Inter alia, the circle of reporting entities was significantly widened by Act 367/2000 and a regime of sanctions had been created. A significant change was the replacement of the previous "suspicious transaction" reporting system with a regime based on the reporting by obliged entities of "unusual business activity". "Unusual business activity", though defined in the 2000 Act, still raises some problems for the examiners discussed below. Since the on-site visit, Act 367/2000 has itself been amended by Act 445/2002, which came into force on 1 September 2002. The 2002 Act was aimed, inter alia, at bringing the preventive regime into line with Directive 2001/97/EC and, together, these two acts now provide a basically sound preventive legal structure. The challenge is now to operationalise these laws. Issues relating to these acts are further considered beneath in relation to the preventive regime in the financial sector as a whole.

5. On the legal repressive side, a major development was the ratification of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime ("the Strasbourg Convention") in May 2001, and which was brought into force in September 2001.

6. Some amendments were also made to the money laundering offence, notably the removal of the financial threshold. The mental element of the offence, however, remains the knowledge standard and a lesser subjective mental element should be considered to assist the prosecutorial regime (such as suspicion with lesser penalties). Money laundering by negligence was not being actively pursued at the time of the on-site visit and the examiners urge, once again, its consideration in appropriate circumstances.

7. 39 prosecutions for money laundering were reported since the adoption of the first report and a modestly encouraging number of convictions had been achieved up to the time of the on-site visit (9). It was understood that most, if not all, of those convictions arose out of cases where there were also prosecutions for the underlying predicate offences. These predicate offences were exclusively related to theft of motor vehicles from abroad. There had been no money laundering convictions arising out of drugs or corruption cases. No convictions were reported for money laundering as a "stand alone" offence or in the absence of a conviction for the predicate offence. Given the high number of drug trafficking, fraud and corruption offences investigated, the examiners were concerned that few, if any, money laundering cases had arisen out of such important proceeds-generating cases. The effectiveness therefore of the overall law enforcement response to money laundering was seriously questioned. Despite the training that had been given to law enforcement on the issue and the growth of prosecutor specialisation, the examiners consider that still greater efforts need to be made to follow the proceeds of crime in major proceeds-generating investigations, with a view to more money laundering prosecutions being brought, particularly where professional launderers are acting on behalf of third parties and/or organised crime groups, and where it may not be possible to prosecute an offender for the underlying predicate crime. Clear guidelines need to be drawn up as to the minimum evidential requirements to launch money laundering prosecutions. Similarly, major confiscation orders need to be achieved. No confiscation orders were reported in respect of any of the money laundering convictions, which was disappointing.

8. Though the police have broadly satisfactory investigative powers, including a range of most special investigative techniques, a more proactive use of them, together with a greater emphasis on modern financial investigative techniques would be beneficial. Controlled delivery of cash proceeds needs clearly providing for in the law.

9. There have been no changes to the regime of provisional measures and confiscation since the first report. The legal regime retains the same ambiguities, uncertainties and lack of clarity as at the time of the first evaluation. No confiscation statistics were provided in answer to the second mutual evaluation questionnaire and the examiners were left with the impression that confiscation was seldom used. It was impossible to make value confiscation orders domestically in respect of property legally obtained and this needs clearly providing for. Equally, confiscation of income and benefits from illegal property also appeared problematical . If real progress is to be made in dismantling the economic basis of organised crime, then a robust legal regime, which allows for the making of serious and dissuasive confiscation orders is vital. The examiners therefore endorse the recommendations made in the first round and strongly urge the Slovak authorities to carefully review the legal framework to ensure that they have a comprehensive set of provisional measures and forfeiture /confiscation provisions, which facilitate the tracing, freezing and seizing of instrumentalities and criminal proceeds (as widely defined in the Strasbourg Convention) with a view to eventual confiscation orders, and which clearly allows for confiscation orders at the conclusion of criminal proceedings in respect of instrumentalities, and direct and indirect proceeds or property, the value of which corresponds to such proceeds. The Slovakian authorities should also consider the reversal of the burden of proof post-conviction to assist the court in identifying criminal proceeds liable to confiscation in appropriate cases. Moreover, a judicial culture needs to be developed in which confiscation orders are made routinely in relation to significant criminal proceeds post conviction.

10. So far as international co-operation is concerned, at the time of the first evaluation, Slovakia was not in a position to enforce foreign judgements on confiscation orders and orders for provisional measures. These major deficiencies have now been remedied though no requests for enforcement have,

as yet, been made. The FIU, in particular, is an active member of the Egmont Group and is engaging effectively in the provision of international assistance to other foreign authorities. There still remains no possibility of sharing confiscated assets with other states. The examiners consider that Slovakia should empower its authorities, by legislation or otherwise, to share confiscated assets.

11. On the preventive side, the two new anti-money laundering laws create a wide range of entities that have anti-money laundering reporting obligations and customer identification obligations in respect of "business activities" exceeding 15 000 Euros. The range of reporting entities is in line with Directive 2001/97/EC. The recognition of "unusual business activity", without further clarification in the law or general indicators as to what may amount to unusual business activity may be problematical. It was not clear to the examiners whether this regime was limited entirely to business/trade activities and excludes transactions on accounts of a personal nature. The Slovak authorities may now wish to review the operation of the new legislation to ensure that the creation of the new obligations has not inadvertently limited the scope of the reporting obligation. In any event, meaningful guidance needs to be prepared for each sector as to what may amount to "unusual business activity", and the examiners consider that the creation of such guidance needs to be co-ordinated, rather than rely on each bank or obliged entity to create its own indicators. At the time of the on-site visit, the banks remained the major reporter. Since the adoption of the first round report until 30 September 2001 the FIU received 1223 reports from banks, and it was understood 80% of the banks were reporting. Under-reporting banks need to be known to the National Bank of Slovakia (NBS). At the time of the on-site visit, reports from the non-banking sector were modest:

- Insurance companies: 7
- Securities centre: 17
- Leasing companies: 1
- Others: 2

12. There were no reports from casinos and exchange houses. Thus, at the time of the on-site visit, much work still needed to be done to develop real awareness of these issues outside the banking sector. The FIU has a major role in outreach and developing appropriate systemised feedback arrangements to all players in the financial sector.

13. The FIU is working effectively in analysing the information it receives and is generating a significant flow of reports to law enforcement. It was unclear how many money laundering cases were generated by the police outside of the reporting regime, and statistics on this would be useful. The FIU is vested with large responsibilities for supervision of compliance by virtue of Art. 10 of Act 367 and the FIU needs to be resourced accordingly. Prudential supervision over the banks is now exclusively vested in the NBS. The Ministry of Finance has the responsibility for casinos, and the Financial Markets Authority, created in November 2000 is responsible for the supervision of the capital market and insurance. At the time of the on-site visit, it was considered that the division of responsibilities between the prudential supervisors and the FIU needed clarification and various memoranda of understanding have since been signed. That said, at the time of the on-site visit, supervision outside the banking sector was in its infancy, and the prudential supervisors still remained too distanced from the anti-money laundering issue (which was a concern in the first report). They all need to include anti-money laundering supervision in their on-site inspections and the non-banking prudential supervisors' awareness of the dangers from money laundering needed raising, particularly in the Financial Markets Authority. All obliged entities need the role and responsibilities of compliance officers clarified.

14. The NBS exercises a generally strong licensing and monitoring regime for the banks, but the examiners were less certain about the regime for exchange houses. The NBS has, since 2000, begun to develop a more proactive anti-money laundering inspection regime (in 2002, there were 3 anti-money laundering inspections in larger banks). However, there were no substantial changes in the NBS' supervision over the exchange houses so far as anti-money laundering issues were concerned, and a thorough inspection regime needs to be in place, given the large role that cash still plays in the

economy. The licensing regime outside the banking sector could be improved. In the insurance and securities sectors and in the licensing of casinos, the origin of capital needs greater investigation.

15. Neither Law 367/2000, now Law 445/2002, covers customer identification on the establishment of a business relationship. If not covered elsewhere, it should be. Equally, the reporting obligations in the laws should also be applicable to the NBS.

16. It is clear that there is within the Slovak Republic a political will to remove bearer passbooks in their entirety. The removal is a graduated process. As form 1 January 2007, bearer passbooks will no longer exist.

17. There have been significant developments in the identifications of beneficial owners of transactions. The new Banking Law (483/2001) provided that a bank or branch office of a foreign bank is obliged to determine the ownership of funds a client uses in transactions over 15 000 Euros. Ownership of funds shall be determined by a binding written statement of the client in which the client is obliged to declare whether these funds are his property and whether he is conducting the transaction on his own account. A similar rule needed to be extended to obliged entities other than banks in respect of transactions. A similar rule would be helpful when commencing business transactions.

18. Undoubtedly, there has been considerable progress overall by Slovakia, for which credit is given. But it is still difficult to judge the overall effectiveness of the system, particularly in the absence of statistics in many areas. The jurisdiction would benefit from some defined performance indicators, periodically monitored by an overarching steering group. More work still needs to be done on the preventive side to generate reports from the vulnerable sectors beyond banking and active supervision needs developing further outside the banking sector. More focus on the repressive side on the pursuit of proceeds is critical. With greater emphasis on these issues, Slovakia can develop the effectiveness of its anti-money laundering structures even further.

ANNEX F

SUMMARIES OF MUTUAL EVALUATIONS UNDERTAKEN BY THE OFFSHORE GROUP OF BANKING SUPERVISORS (OGBS)

Gibraltar[1]

1. Gibraltar has in place a robust arsenal of legislation, regulations and administrative practices to counter money laundering. The authorities clearly demonstrate the political will to ensure that their financial institutions and associated professionals maximise their defences against money laundering, and cooperate effectively in international investigations into criminal funds. Gibraltar is close to complete adherence with the FATF 40 Recommendations. Once the appropriate changes are made to the few remaining deficient areas, these standards will be fully met.

2. Gibraltar has a comprehensive legal framework in place for preventing and combating money laundering. Gibraltar ratified the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in 1994, and, in 1996, extended its legislation on money laundering to all serious crimes. The money laundering offences are broad, and cover a wide range of offences (all offences with a maximum of over one year imprisonment). There is a requirement to report suspicious transactions, backed up with effective measures to prevent tipping off, and to provide the necessary protections to those who submit reports.

3. Current law places significant constraints on cooperation between Gibraltar and other jurisdictions in relation to non-drug related money laundering offences. Despite these constraints, Gibraltar authorities have a good record of cooperation with overseas requests for assistance, on both regulatory and criminal matters. The wide range of predicate offences in Gibraltar law should prevent the requirement for dual criminality from hindering cooperation, including cases involving tax crimes. The evaluators recommend the enactment of the proposed Mutual Legal Assistance Law as soon as possible. Once the proposed Law is enacted, Gibraltar will be able to cooperate with foreign enquiries on the full range of money laundering issues. It will allow information to be exchanged with foreign authorities (administrative, law enforcement and judicial) at the intelligence-gathering, investigation and prosecution stages in respect to all criminal offences.

4. The degree to which Gibraltar's financial institutions are used to launder the proceeds of crimes committed locally appears to be small. Because of the nature of the financial business conducted in Gibraltar, few of its financial institutions (with the exception of those serving the local community) routinely take cash deposits. However, cash placements and the exchange of that cash through the fairly unregulated bureaux de change could pose a fairly substantial risk of money laundering. In addition to its powers to seize currency believed to be drug proceeds, Customs should be provided with the powers to seize cash on an all-crimes basis, apply random checks, and monitor the need for additional measures. Regarding the laundering of proceeds from crimes committed outside Gibraltar, there is no evidence of major or systematic money laundering taking place in Gibraltar.

5. The Financial Services Commission (FSC) is responsible for the licensing, supervision and regulation of financial services providers operating in or from within Gibraltar. This includes banks, insurance companies, investment firms, insurance intermediaries, company managers, professional trustees, and insurance company managers. Gibraltar has adequate rules for the regulation and supervision of its financial institutions, with the exception of bureaux de change, which are licensed by the Financial and Development Secretary and are not supervised by the FSC. Although the Gibraltar authorities report that Customs visits the bureaux de change at least annually to ensure compliance with anti-money laundering requirements, the Evaluation Team feels that the fact that bureaux de change are not supervised by the FSC is a source of concern.

[1] Evaluation undertaken in 2001 by a team of officials drawn from the United States, Portugal and Jersey.

6. There are adequate customer identification requirements. Subsequent to the on-site visit to Gibraltar, the Anti-Money Laundering Guidance Notes have been amended and reliance on third parties to conduct "know your customer" procedures regarding customers (introducer certificates) has been severely limited. The Evaluation Team welcomes the amendments made and finds them satisfactory. Regarding client accounts held by legal professionals and other intermediaries, such as stock brokers, fund managers, accountants, and estate agents, although the before-mentioned persons or entities must know their clients and are liable for account activity, the Evaluation Team recommends that, in accordance with FATF Recommendations 11 and 14, at least the nature of the activity to be conducted by the intermediary, on behalf of its customer, through the account, should be disclosed to the institution opening the account.

7. Although financial institutions must report suspicious transactions to the police, Customs, and the GFIU, the police do not have the power to compel production of financial and bank account records in the investigation stage without a court order. Currently, if a bank or other financial institution makes a disclosure under the Criminal Justice Ordinance, then the police can only invite the financial institution to show them the relevant account records and documentation. The relevant authorities indicated that there is a close relationship with the industry and advised that information can be obtained from banks, trusts, companies and other institutions, on a voluntary basis. However, the Evaluation Team feels that it should be made mandatory, by law, for financial institutions to provide information and records to the authorities, when money-laundering cases are being investigated. A power to compel production of records is required. This would be an invaluable investigatory tool for the law enforcement authorities and it would protect financial institutions providing the information.

8. There were 220 suspicious transaction reports filed with the Gibraltar Financial Intelligence Unit (GFIU) in 2000. The overall number of disclosures is encouraging. There has been a careful analysis of the type of institution making disclosures reflecting very few disclosures by professionals. To remedy this imbalance, liaison between the law enforcement agencies and the professional associations could include inviting those associations to educate their members as to their responsibilities under the legislation.

9. There is no statutory authority gateway at present for the GFIU to share information with external income tax authorities. There is a government commitment to the OECD to exchange information on criminal and civil tax matters.

10. There is an informal relationship between the FSC and the GFIU; the heads of the two entities meet regularly and share information. Both the GFSC and the GFIU considered the system works well. The Evaluation Team recommends establishment of a more formal group charged with analysing trends in reporting and the issues raised by particular cases to enable strategies to be developed on how to meet challenges posed by emerging trends.

11. Gibraltar authorities report that while there are no central records kept of the number of international requests received and acceded to, the Royal Gibraltar Police, Customs, and the Attorney General's Chambers each maintain their own records of such requests. Until October 2001, no records were kept by the Attorney General's Chambers. However, recently, data on requests received has begun to be collated by the Attorney General's Chambers. Such information will provide an important statistical tool regarding the level of co-operation given to the international community.

12. The Evaluation Team considers that Gibraltar has established a comprehensive anti-money laundering system, and that adoption of the proposals contained in this mutual evaluation report will ensure that it complies with the best international anti-money laundering standards. Finally, the Evaluation Team would like to again express its appreciation to the authorities of Gibraltar for the constructive manner in which they participated in the mutual evaluation process.