In case of discrepancies between the French and the English texts, the French text shall prevail

Luxembourg, 1st July 2003

To all the persons and entities
supervised by the CSSF

CSSF CIRCULAR 03/104

Re: **Supplement to CSSF Circulars 00/16, 01/31, 01/37, 01/48, 02/66, 02/73, 03/86, 03/93 and IML 94/112 regarding the fight against money laundering and the prevention of the use of the financial sector for money-laundering purposes**

Dear Sir, Madam,

1) We are pleased to inform you that the Financial Action Task Force on Money Laundering (FATF) published its updated report on non-cooperative countries and territories (NCCTs) in the fight against money laundering on 20 June 2003.

The members of FATF decided to remove **St Vincent and the Grenadines** from the NCCT list following the legislative and regulatory efforts made by this country as regards the fight against money laundering. The list of NCCTs is consequently comprised of the following jurisdictions: **Cook Islands, Egypt, Guatemala, Indonesia, Myanmar, Nauru, Nigeria, Philippines and Ukraine**.

We remind all the professionals of the financial centre to remain particularly vigilant as regards clients and financial transactions involving one of the countries listed on the updated FATF list. The principles laid down in CSSF Circular 00/16 continue to apply.

2) We also draw your attention to the adoption of the revised Forty Recommendations against money laundering at the plenary meeting of FATF in June 2003 (cf. Annexes).

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Arthur PHILIPPE
Director

Jean- Nicolas SCHAUS
Director General

Annexes.

Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

Annual Review of Non-Cooperative Countries or Territories

20 June 2003

NCCT2003_en.doc//21.06.2003/11h00

TABLE OF CONTENTS

EXECUTIVE SUMMARY OF THE JUNE 2003 NCCTS REPORT

1. In order to reduce the vulnerability of the international financial system, increase the world-wide effectiveness of anti-money laundering measures, and recognise progress made in these areas, the FATF agreed to the following steps:

Removal of countries from the Non-Cooperative Countries and Territories (NCCTs) list in October 2002, February 2003, and June 2003

- It recognises that St. Vincent and the Grenadines, listed as non-cooperative in the fight against money laundering in June 2000, has sufficiently addressed the deficiencies identified by the FATF through enactment and implementation of appropriate legal reforms. In October 2002, the Plenary recognised that Russia, Dominica, Niue and Marshall Islands, identified as NCCTs in June 2000, had addressed the identified deficiencies and therefore removed them from the NCCTs list. And in February 2003, the Plenary removed Grenada from the list of NCCTs after enactment and implementation of legal reforms addressing identified deficiencies. Consequently, the procedures prescribed in FATF Recommendation 21 are withdrawn. To ensure continued effective implementation of these reforms, the FATF will monitor the developments in St. Vincent & the Grenadines, as well as Dominica, Niue, the Marshall Islands, and Grenada, in consultation with the relevant FATF-style regional body and particularly in the areas laid out in this NCCT report.

- Although removed from the NCCTs list in June 2001, the Bahamas has been subject to FATF monitoring since that time. The FATF encourages the Bahamas to improve mechanisms for international co-operation so that the FATF may end formal monitoring.

Progress made since June 2002

- It welcomes the progress made by the Cook Islands, Egypt, Guatemala, Nigeria, the Philippines, Ukraine and Nauru in addressing deficiencies and calls upon them to continue this work. Until the deficiencies have been fully addressed and the necessary reforms have been sufficiently implemented, it believes that scrutiny of transactions with these jurisdictions, as well as those with Indonesia and Myanmar, continues to be necessary and reaffirms its advice of June 2000 to apply, in accordance with Recommendation 21, special attention to such transactions. The FATF notes with particular satisfaction that Egypt, Guatemala, and the Philippines have enacted most, if not all legislation needed to remedy the deficiencies previously identified. On the basis of this progress, the FATF will invite those countries to submit implementation plans to enable the FATF to evaluate actual implementation of the legislative changes in each jurisdiction according to the principles agreed upon by its Plenary.

- With respect to jurisdictions de-listed in June 2002 and subject to the monitoring process from June 2002—June 2003, future monitoring for St Kitts & Nevis will be conducted within the context of the Caribbean Financial Action Task Force's (CFATF) relevant monitoring mechanisms. Future monitoring of Hungary will be conducted within the Council of Europe's MONEYVAL and its relevant monitoring mechanisms.

Counter-measures

- Due to Ukraine's failure to enact anti-money laundering legislation that met international standards, the Plenary recommended that counter-measures apply to Ukraine as of 20 December 2002. However, after that time, Ukraine enacted legislation that significantly addressed the identified deficiencies, and therefore the FATF Plenary removed the application of counter-measures on 14 February 2003. Due to Nauru's failure to enact appropriate legislative measures and the existence of numerous shell banks, counter-measures have been in effect with respect to Nauru since

December 2001. The FATF welcomes Nauru's recent legislative measures to eliminate shell banks. The FATF would like Nauru to take additional steps to ensure that previously licensed offshore banks are no longer conducting banking activity and are no longer in existence. When it is shown that Nauru has fully co-operated with the international community and has taken every step to ensure that shell banks no longer operate, the FATF can consider the removal of counter-measures.

Jurisdictions that have not made adequate progress

- It noted with concern the failure by the governments of Indonesia and Myanmar to enact significant reforms since June 2002 to address their remaining deficiencies. The FATF strongly urges them to prioritise the enactment and enforcement of the needed reforms by the next FATF Plenary meeting.

2. With respect to those countries on the NCCTs list whose progress in addressing deficiencies has stalled, the FATF will consider the adoption of additional counter-measures as well.

3. In sum, the list of NCCTs is comprised of the following jurisdictions: **Cook Islands; Egypt; Guatemala; Indonesia; Myanmar; Nauru; Nigeria; Philippines; and Ukraine**. The FATF calls on its members to update their advisories requesting that their financial institutions give special attention to businesses and transactions with persons, including companies and financial institutions, in those countries or territories identified in the report as being non-cooperative.

INTRODUCTION AND BACKGROUND

4. The Forty Recommendations of the Financial Action Task Force (FATF) have been established as the international standard for effective anti-money laundering measures. FATF regularly reviews its members to check their compliance with these Forty Recommendations and to suggest areas for improvement. It does this through annual self-assessment exercises and periodic mutual evaluations of its members. The FATF also identifies emerging trends and methods used to launder money and suggests measures to combat them.

5. Combating money laundering is a dynamic process because the criminals who launder money are continuously seeking new ways to achieve their illegal ends. It has become evident to the FATF through its regular typologies exercises that, as its members have strengthened their systems to combat money laundering, the criminals have sought to exploit weaknesses in other jurisdictions to continue their laundering activities.

6. In order to reduce the vulnerability of the international financial system to money laundering, governments must intensify their efforts to remove any detrimental rules and practices that obstruct international co-operation against money laundering. The goal of the FATF's work in this area is therefore to secure the adoption by all financial centres of international standards to prevent, detect and punish money laundering.

7. In this context, on 14 February 2000, the FATF published an initial report on the issue of non-cooperative countries and territories (NCCTs)[1], which set out twenty-five criteria identifying detrimental rules and practices that impede international co-operation in the fight against money laundering (see Appendix). The criteria are consistent with the FATF Forty Recommendations. It describes a process whereby jurisdictions having such rules and practices can be identified and encourages these jurisdictions to implement international standards in this area. Finally, the report contains a set of possible counter-measures that FATF members could use to protect their economies against the proceeds of crime.

8. A major step in this process was the publication of the June 2000 Review[2] and June 2001 Review[3] to identify non-cooperative countries or territories, and the September 2001 news release[4], which identified a total of 23 NCCTs. This initiative has so far been both productive and successful because most of these jurisdictions have made significant and rapid progress, with 14 being removed from the NCCTs list as of 20 June 2003. The June 2002 NCCT Review[5] updates the situation as of that time. No additional jurisdictions were reviewed since that time.

9. The FATF approved this report at its 18-20 June 2003 Plenary meeting. Section I of this document summarises the review process. Section II highlights progress made by the jurisdictions deemed to be non-cooperative in June 2000, June 2001, and September 2001 that remained on the NCCTs list prior to the June 2003 Plenary meeting. Section III updates the situations in de-listed jurisdictions that were subject to the monitoring process from June 2002 – June 2003. Section IV concludes the document and indicates future steps.

---

1 Available at the following website address: http://www.fatf-gafi.org/pdf/NCCT_en.pdf

2 Available at the following website address: http://www.fatf-gafi.org/pdf/NCCT2000_en.pdf

3 Available at the following website address: http://www.fatf-gafi.org/pdf/NCCT2001_en.pdf

4 Available at the following website address: http://www.fatf-gafi.org/pdf/PR-20010907_en.pdf

5 Available at the following website address: http://www.fatf-gafi.org/pdf/NCCT2002_en.pdf

I. PROCESS

10. At its February 2000 Plenary meeting, the FATF set up four regional review groups (Americas; Asia/Pacific; Europe; and Africa and the Middle East) to analyse the anti-money laundering regimes of a number of jurisdictions against the above-mentioned twenty-five criteria. In 2000-2003, the review groups were maintained to continue this work and to monitor the progress made by NCCTs.

A. REVIEW PROCESS

11. The jurisdictions to be reviewed were informed of the work to be carried out by the FATF. The reviews involved gathering the relevant information, including laws and regulations, as well as any mutual evaluation reports, related progress reports and self-assessment surveys, where these were available. This information was then analysed against the twenty-five criteria and a draft report was prepared and sent to the jurisdictions for comment. In some cases, the reviewed jurisdictions were asked to answer specific questions designed to seek additional information and clarification. Each reviewed jurisdiction provided their comments on their respective draft reports. These comments and the draft reports themselves were discussed between the FATF and the jurisdictions concerned during a series of face-to-face meetings. Subsequently, the draft reports were discussed and adopted by the FATF Plenaries. The findings are reflected in Sections II and III of the present report. For NCCTs, FATF has indicated that Recommendation 21[6] applies.

B. ASSESSING PROGRESS

12. The assessments of the jurisdictions identified as non-cooperative by the FATF were discussed as a priority item at each FATF Plenary meeting during 2002-2003. These assessments were discussed initially by the FATF review groups, including through face-to-face meetings, and then discussed by the FATF Plenary.

13. Decisions to revise the NCCTs list are taken in the FATF Plenary. In deciding whether a jurisdiction should be removed from the list, the FATF Plenary assesses whether a jurisdiction has adequately addressed the deficiencies previously identified. The FATF views the enactment of the necessary legislation and the promulgation of associated regulations as essential and fundamental first step for jurisdictions on the list. The FATF attaches particular importance to reforms in the area of criminal law, financial supervision, customer identification, suspicious activity reporting, and international co-operation. Legislation and regulations need to have been enacted and to have come into effect before removal from the list can be considered.

14. In addition, the FATF seeks to ensure that the jurisdiction is effectively implementing the necessary reforms. Thus, the jurisdictions which have enacted most, if not all legislation needed to remedy the deficiencies were asked to submit implementation plans to enable the FATF to evaluate the actual implementation of the legislative changes according to the above principles. Information related to institutional arrangements, as well as the filing of suspicious activity reports, examinations of financial institutions, international co-operation and the conduct of money laundering investigations, are

[6] 21. Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these 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 supervisors, auditors and law enforcement agencies.

considered. Finally, the FATF has further elaborated a process, which includes on-site visits to the jurisdiction concerned, by which jurisdictions can be de-listed at the earliest possible time. (See Annex.)

C. MONITORING PROCESS FOR JURISDICTIONS REMOVED FROM THE NCCT LIST

15. To ensure continued effective implementation of the reforms enacted, the FATF has adopted a monitoring mechanism to be carried out in consultation with the relevant FATF-style regional body. This mechanism includes the submission of regular implementation reports and a possible follow-up visit to assess progress in implementing reforms and to ensure that stated goals have, in fact, been fully achieved.

16. The monitoring process of de-listed jurisdictions will be carried out against the implementation plans already submitted by de-listed jurisdictions, specific issues raised in the updated reports, and the experience of FATF members on implementation issues. In this context, subjects addressed may include, as appropriate: the issuance of secondary legislation and regulatory guidance; inspections of financial institutions planned and conducted; STR systems; process for money laundering investigations and prosecutions conducted; regulatory, FIU and judicial co-operation; adequacy of resources; and assessment of compliance culture in the relevant sectors.

D. IMPLEMENTATION OF COUNTER-MEASURES

17. In jurisdictions that have failed to make adequate progress in addressing the serious deficiencies previously identified by the FATF, in addition to the application of Recommendation 21, the FATF recommends the application of further counter-measures which should be gradual, proportionate and flexible regarding their means and taken in concerted action towards a common objective. The FATF believes that enhanced surveillance and reporting of financial transactions and other relevant actions involving these jurisdictions would now be required, including the possibility of:

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;

- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;

- In considering requests for approving the establishment in FATF member countries of subsidiaries or branches or representative offices of banks, taking into account the fact that the relevant bank is from an NCCT;

- Warning non-financial sector businesses that transactions with entities within the NCCTs might run the risk of money laundering.

II. FOLLOW-UP TO JURISDICTIONS ON THE NCCT LIST

18. This section constitutes an overview of progress made by these jurisdictions. Jurisdictions marked with an asterisk are still regarded as being non-cooperative by the FATF. (References to "meeting the criteria" means that the concerned jurisdictions were found to have detrimental rules and practices in place.) For each of the following jurisdictions, the situation which prevailed when the jurisdiction was place on the NCCTs list is summarised (criteria met, main deficiencies) and is followed by an overview of the actions taken by jurisdictions since that time.

A. JURISDICTIONS THAT ARE NO LONGER CONSIDERED AS NON-COOPERATIVE

St. Vincent and the Grenadines

Situation in June 2000

19. In June 2000, St. Vincent and the Grenadines met criteria 1-6, 10-13, 15, 16 (partially), 18, and 22-25. There were no anti-money laundering regulations or guidelines in place with respect to offshore financial institutions, and thus no customer identification or record-keeping requirements or procedures. There was no system to require reporting of suspicious transactions. IBC and trust law provisions created additional obstacles, and international judicial assistance was unduly limited to situations where proceedings had been commenced against a named defendant in a foreign jurisdiction.

Progress made since June 2000

20. St. Vincent and the Grenadines has enacted significant legislative reforms to address the deficiencies identified in June 2000, including the Proceeds of Crime and Money Laundering (Prevention) Act No. 39 of 2001, of 18 December 2001 (amended 28 May 2002), and the Proceeds of Crime (Money Laundering) Regulations 2002 of 29 January 2002 (amended 26 April 2002). These provisions criminalise the laundering of proceeds from any criminal conduct, mandate record keeping requirements for on-shore and offshore institutions, and mandate suspicious transaction reporting. The Financial Intelligence Unit Act, No. 38 of 2001, creates an FIU. Amendments to the International Banks Act (No. 7 of 2000 and no. 30 of 2002) improve registration requirements for offshore banks, and the Exchange of Information Act n° 29 of 2002, of June 2002, expands regulatory co-operation and repeals the previously restrictive Confidential Relationships Preservation (International Finance) Act.

21. The Eastern Caribbean Central Bank (ECCB), in conjunctions with local supervisory authorities, now supervises St. Vincent and the Grenadines' offshore banks. Exchange of Information order, 2002 no. 48, effective 5 November 2002, also expands the ECCB's authority to share information regarding on-shore financial institutions.

22. St. Vincent and the Grenadines has also taken adequate steps to implement these reforms. Since June 2000, the size of the offshore sector has also been significantly reduced. In the future, the FATF encourages strengthening the oversight of offshore entities and continued judicial, regulatory, and FIU co-operation. The FATF also encourages St. Vincent and the Grenadines to consider tightening provisions relating to the granting of exemptions from customer identification requirements.

B. JURISDICTIONS THAT HAVE MADE PROGRESS SINCE JUNE 2002

Cook Islands *

Situation in June 2000

23. In June 2000, the Cook Islands met criteria 1, 4, 5, 6, 10, 11, 12, 14, 18, 19, 21, 22, 23 and 25. In particular, the Government had no relevant information on approximately 1,200 international companies that it had registered. The country also licensed offshore banks that were not required to identify customers or keep their records and were not effectively supervised. Excessive secrecy provisions guarded against the disclosure of relevant information on those international companies as well as bank records.

Progress made since June 2000

24. In August 2000 the Cook Islands Parliament enacted the "Money Laundering Prevention Act 2000" (MLPA). Guidance notes for financial institutions on the prevention of money laundering were issued by the Money Laundering Authority (MLA) in mid-2001 and on 23 January 2002, the Cook Islands passed the Money Laundering Prevention Regulations 2002 (the regulations), pursuant to section 41 of the Act. A financial intelligence unit (FIU) was established under a Letter of Delegation in respect of certain of the powers of the MLA under section 9 (1) (a), (e), (f), (g), and (h) of the MLPA.

25. On 7 May 2003, the Cook Islands took significant steps by passing nine new Acts. They include the Crimes Amendment Act 2003; the Proceeds of Crime Act 2003; Mutual Assistance In Criminal Matters Act 2003; the Financial Transactions Reporting Act 2003, (FTRA); the Financial Supervisory Commission Act 2003, (FSCA); the Banking Act 2003; and the International Companies Amendment Act 2003 (ICAA). The legislation creates measures for an overall comprehensive anti-money laundering framework and introduces regulation and supervision of the financial sector consistent with international standards. However, the necessary regulations under the acts have to be promulgated.

26. The FATF welcomes these substantial new measures and the fact that they will eliminate the existence of shell banks in the Cook Islands by 1 June 2004. The FATF emphasises the need for early and effective implementation, as the continued existence of shell banks is considered to reduce the effectiveness of an anti-money laundering regime and poses an unacceptable risk to the international financial community.

Egypt *

Situation in June 2001

27. In June 2001, Egypt met criteria 5, 10, 11, 14, 19 and 25, and it partially met criteria 1, 6 and 8. Particular concerns identified included: a failure to adequately criminalise money laundering to internationally accepted standards; a failure to establish an effective and efficient STR system covering all financial institutions; a failure to establish an FIU or equivalent mechanism; and a failure to establish rigorous identification requirements that apply to all financial institutions. Further clarification was also sought on the evidential requirements necessary for access to information covered by Egypt's banking secrecy laws.

Progress made since June 2001

28. On 22 May 2002, Egypt enacted Law No. 80-2002 for Combating Money Laundering. The law criminalises the laundering of proceeds from various crimes, including narcotics, terrorism, fraud, and organised crime. The law addresses customer identification, record-keeping, and establishes the framework for the Money Laundering Combating Unit (MLCU) to function as an FIU within the

Central Bank of Egypt. On 24 June 2002, Presidential Decree No. 164 of 2002 was issued which formally established and structured the MLCU.

29. Law no. 78-2003 came into effect 9 June 2003. It enhances the scope of the Law No. 80-2002 by expanding the predicate offences and removing a previous loophole which appeared to grant broad exemptions from imprisonment. Prime Minister Decree No. 951-2003 details the Executive Regulations for Law No. 80-2002 and came into effect on 10 June 2003. The Regulations further detail anti-money laundering obligations for financial institutions, including banks, bureaux de change, money remittance, securities, and insurance. The Regulations detail requirements for STR reporting, customer identification procedures, the functions of the MLCU, supervision of entities for compliance with the obligations, and international co-operation.

Guatemala *

Situation in June 2001

30. In June 2001, Guatemala met criteria 6, 8, 15, 16, 19 and 25 and partially met criteria 1, 7 and 10. Guatemalan laws contained secrecy provisions that constituted a considerable obstacle to administrative counter-money laundering authorities, and Guatemalan law provided no adequate gateways for administrative authorities to co-operate with foreign counterparts. Additionally, Guatemala had not criminalised money laundering beyond the proceeds of narcotics violations. Further, the suspicious transaction reporting system contains no provision preventing "tipping off." Guatemala had recently issued Regulations for the Prevention and Detection of Money Laundering, which significantly improved Guatemala's ability to implement customer identification procedures.

Progress made since June 2001

31. Guatemala enacted Decree No. 67-2001, "Law Against Money and Asset Laundering," on 27 November 2001. The law criminalises the laundering of proceeds relating to any crime, contains specific record-keeping requirements, and creates a special investigative unit (IVE) as a financial intelligence unit. The law's April 2002 implementing regulations improve suspicious transaction reporting and customer identification requirements. Decree No. 19-2002, the Banks and Financial Groups Law, of 1 June 2002, will place offshore banks under the oversight of the Superintendent of Banks (SIB) after a six-month transition period following application for authorisation to operate. In addition, on 21 May 2003, the Monetary Board issued Resolution JM-68-2003, which requires banks to cancel or register all existing coded accounts within 3 months.

32. Although the SIB has conducted on-site inspections of 13 offshore banks (12 of which have applied for authorisation), the SIB has not completed the licensing and authorisation process. These entities therefore continue to operate without adequate supervision. Guatemala is encouraged to complete the authorisation process and bring these entities under the full control of the SIB as promptly as possible.

Nigeria*

Situation in June 2001

33. Nigeria demonstrated an unwillingness or inability to co-operate with the FATF in the review of its system, and when placed on the NCCTs list in June 2001, met criteria 5, 17 and 24. It partially met criteria 10 and 19, and had a broad number of inconclusive criteria as a result of its general failure to co-operate in this exercise.

Progress made since June 2001

34. The Government of Nigeria has substantially improved its co-operation with the FATF and it willingness to address its anti-money laundering deficiencies. On 14 December 2002, Nigeria enacted

the Money Laundering Act (Amendment) Act 2002. This Act significantly enhanced the scope of Nigeria's 1995 Money Laundering Law by extending predicate offences for money laundering from drugs to "any crime or illegal act," extending certain anti-money laundering obligations to non-bank financial institutions, and extending customer identification requirements to include occasional transactions of $5,000 or more. In December 2002, Nigeria also enacted the Economic and Financial Crime Commission (Establishment) Act. Once established, the Commission to will enforce anti-money laundering provisions and investigate alleged offences. The Banking and other Financial Institutions (BOFI) Amendment Act, also enacted in December 2002, improves licensing requirements for financial institutions.

35. Nigeria enacted the Money Laundering Act 2003 on 22 May 2003. It consolidates and supersedes the previous anti-money laundering legislation. It provides for a broader interpretation of financial institutions and scope of supervision of regulatory authorities on money laundering activities, and improves customer identification requirements. It also improves STR provisions by removing a previous threshold.

36. Nigeria is encouraged in its efforts to strengthen and harmonise domestic laws and entities and put the new measures into full effect. Nigeria has created an Economic and financial Crimes Commission, which will receive STRs and function as an FIU, but it is not yet fully operational.

The Philippines*

Situation in June 2000

37. In June 2000, the Philippines met criteria 1, 4, 5, 6, 8, 10, 11, 14, 19, 23 and 25. The country lacked a basic set of anti-money laundering regulations such as customer identification and record keeping. Bank records had been under excessive secrecy provisions. It did not have any specific legislation to criminalise money laundering per se. Furthermore, a suspicious transaction reporting system did not exist in the country.

Progress made since June 2000

38. The Anti-Money Laundering Act (AMLA) of 2001 was enacted on 29 September 2001 and took effect 17 October 2001. The Act criminalises money laundering, introduces the mandatory reporting of certain transactions, requires customer identification, and creates the legal basis for the Anti-Money Laundering Council (AMLC), which functions as an FIU. The Act's implementing rules and regulations (IRRs) took effect 2 April 2002. Although the Philippines' authorities interpreted the regulations as requiring the reporting of all suspicious transactions, this nevertheless conflicted with the AMLA, which only required reporting of high threshold suspicious transactions. A legislative measure was needed to address this issue.

39. On 7 March 2003, the Philippines enacted Republic Act No. 9194, which amends the AMLA and addresses the legal deficiencies. It requires the reporting of all suspicious transactions, grants the BSP (the banking supervisor) full access to account information to examine for anti-money laundering compliance, and allows the AMLC to inquire into deposits and investments made prior to the AMLA coming into effect. Since the general restrictions on access to information have been deleted from the AMLA, the AMLC may now respond to foreign information requests regarding deposits and investments made prior to the coming into effect of the AMLA. The Philippines will now need to adequately implement the anti-money laundering measures.

Ukraine*

Situation in September 2001

40. In September 2001, Ukraine met criteria 4, 8, 10, 11, 14, 15, 16, 23, 24 and 25. It partially met criteria 1, 2, 3, 5, 6, 7 and 13. The country lacked a complete set of anti-money laundering measures. There was no efficient mandatory system for reporting suspicious transactions to an FIU. Other deficiencies concerned customer identification provisions. There were inadequate resources to combat money laundering.

Progress made since September 2001

41. Ukraine has adopted certain presidential decrees, including: Decree No 1199/2001 (10 December 2001) "On the Measures Aimed at Elimination of Legalisation (Money Laundering) of the Profits Obtained by Illegal Ways), Resolution No. 35 (10 January 2002) "On Establishment of the State Department of Financial Monitoring." Regulation No. 700 (29 May 2002) provides guidance to what kinds of transactions financial institutions should consider as "doubtful and uncommon." However, Ukraine still lacked comprehensive anti-money laundering legislation.

42. The FATF decided that its members apply counter-measures to Ukraine as of 15 December unless Ukraine enacted legislation that met international standards. On 7 December, Ukraine enacted the "Law of Ukraine on Prevention and Counteraction of the Legalisation (Laundering) of the Proceeds from Crime." However, this legislation did not meet international standards, and therefore counter-measures became effective on 20 December 2002. Since that time, however, Ukraine enacted amendments that significantly improved the STR system, measures for information sharing, and identification of beneficial ownership of legal entities. Amendments to the criminal code clarified the money laundering offence. As a result of these new measures, the FATF removed the application of counter-measures on 14 February 2003. Ukraine's new basic anti-money laundering law, with amendments, entered into force on 12 June 2003. However, Ukraine still needs to bring these measures into full effect as well as establish a comprehensive and operational regulatory and supervisory structure for non-bank financial institutions.

C. JURISDICTIONS THAT HAVE NOT MADE ADEQUATE PROGRESS SINCE JUNE 2002

Indonesia*

Situation in June 2001

43. In June 2001, Indonesia met criteria 1, 7, 8, 9, 10, 11, 19, 23 and 25, and partially met criteria 3, 4, 5 and 14. It lacked a basic set of anti-money laundering provisions. Money laundering was not a criminal offence in Indonesia. There was no mandatory system of reporting suspicious transactions to a FIU. Customer identification regulations had been recently introduced, but only apply to banks and not to non-bank financial institutions.

Progress made since June 2001

44. Bank Regulation 3/23/PBI/2001, of 13 December 2001, and Circular Letter of Bank Indonesia, of 31 December 2001, require banks to establish "know your customer" policies, compliance officers, and employee training. On 17 April 2002, Indonesia enacted Law of the Republic of Indonesia Number 15/2002 Concerning Money Laundering Criminal Acts. The law expands customer identification requirements and creates the Indonesian Financial Transaction Reports and Analysis Centre (PPATK), the framework for an FIU. The law criminalises the laundering of illicit proceeds, however, only in relation to criminal proceeds exceeding threshold of 500 million rupiah (approximately USD 60,000 as of June 2003). The law also mandates reporting of suspicious transactions, although the definition of

such transactions is limited. Also, institutions are allowed 14 days to make a report, and the law does not criminalise unauthorised disclosure of such reports. These deficiencies will inhibit adequate domestic anti-money laundering enforcement as well as international co-operation.

45. Although a director of PPATK has been appointed, the unit will not become fully operational until October 2003, when the reporting obligations also become mandatory. In the interim, the Bank of Indonesia has received 178 STRs, referring 19 matters to law enforcement, with one matter before the Attorney General. Decrees number 02/PM/2003 and 45/KMK.06/2003 enhance know your customer provisions for the securities and insurance sectors. However, the remaining regulatory structure for NBFIs remains unclear.

46. Indonesia has drafted legislation that would partly address the remaining issues. Indonesia needs to move quickly to address the deficiencies, especially the removal of the threshold for defining the proceeds of crime, a more comprehensive regulatory framework for non-banking financial institutions, more comprehensive STR requirements, and enhanced measures for international co-operation.

Myanmar*

Situation in June 2001

47. In June 2001, Myanmar met criteria 1, 2, 3, 4, 5, 6, 10, 11, 19, 20, 21, 22, 23, 24 and 25. It lacked a basic set of anti-money laundering provisions. It had not yet criminalised money laundering for crimes other than drug trafficking. There were no anti-money laundering provisions for financial institutions, and there was an absence of a legal requirement to maintain records and to report suspicious or unusual transactions. There were also significant obstacles to international co-operation by judicial authorities.

Progress made since June 2001

48. On 17 June 2002 Myanmar enacted The Control of Money Laundering Law (CMLL) (The State Peace and Development Council Law No. 6 /2002). The law addresses criminalises money laundering for certain predicate offences, including trafficking/smuggling, counterfeiting, and acts of terrorism. This list could be extended, and the law allows for the establishment of a monetary threshold relating to money laundering offences. The law also requires the reporting of suspicious transactions, creates a "safe harbour" provision for reporting, and requires customer identification and record keeping.

49. Although the law creates a framework for anti-money laundering measures, deficiencies remain, and Myanmar has taken little action since June 2002. There are no provisions to enhance international co-operation, particularly mutual legal assistance. Rules that would implement the CMLL still need to be drafted and issued. Also, the law does not criminalise unauthorised disclosure of STRs. In addition, further legislative work may be necessary to fully address the regulatory and supervisory functions of the central bank.

D. JURISDICTIONS CURRENTLY SUBJECT TO COUNTER-MEASURES

Nauru *

Situation in June 2000

50. In June 2000 Nauru met criteria 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 19, 23, 24 and 25. It lacked a basic set of anti-money laundering regulations, including the criminalisation of money laundering, customer identification and a suspicious transaction reporting system. It had licensed approximately 400 offshore "banks," which were prohibited from taking deposits from the public and were poorly supervised. These banks are shell banks that have no physical presence. The excessive secrecy

provisions guarded against the disclosure of the relevant information on those offshore banks and international companies.

Progress made since June 2000

51. On 28 August 2001, Nauru enacted the Anti-Money Laundering Act of 2001. The Act criminalised money laundering, requires customer identification for accounts, and requires suspicious activity reporting. However, the act did not cover the regulation and supervision of Nauru's offshore banking sector; therefore, the FATF recommended that its members apply counter-measures as of 5 December 2001. On 6 December, Nauru amended the law to apply to the offshore banks, however Nauru took no action to address the main area of concern—the licensing and supervision of the offshore sector.

52. Nauru has recently taken steps by enacting the Corporation (Amendment) Act of 2003 and the Anti-Money Laundering Act of 2003 on 27 March 2003. The legislation is intended to abolish offshore shell banks and prohibit the granting of new licences. Nauru has indicated that it has since revoked the licenses of all remaining offshore banks operating out of Nauru and that the only bank currently licensed is the National Bank of Nauru, which conducts only domestic business. While the FATF welcomes these efforts, the FATF would like Nauru to take additional steps to ensure that previously licensed offshore banks are no longer conducting banking activity and are no longer in existence. When it is shown that Nauru has fully co-operated with the international community and has taken every step to ensure that shell banks no longer operate, the FATF can consider the removal of counter-measures.

III. JURISDICTIONS SUBJECT TO THE MONITORING PROCESS

The Bahamas

53. The Commonwealth of the Bahamas was identified as an NCCT in June 2000. The Bahamas subsequently enacted comprehensive anti-money laundering measures, made important progress implementing these measures, and was therefore removed from the NCCTs list in June 2001.

54. The Bahamas established a financial intelligence unit (FIU) that has been successfully operational and was admitted into the Egmont Group in 2001. In 2002, the FIU received 160 STRs and forwarded 45 to the Royal Bahamas Police Force for investigation. The FIU received 49 requests for information from foreign FIUs and responded to 40. From 1 January to 30 April 2003, The FIU received an additional 50 STRs, forwarded 10 for investigation, and had responded to 17 of 28 additional requests for information. To date, there have been 4 convictions under the money laundering legislation, with several other prosecutions on-going.

55. The Bahamas required banks to establish a physical presence in the jurisdiction, and required all pre-existing accounts to be identified by 31 December 2002. The Central Bank also established and began to implement an ambitious inspection programme, conducting 102 on-site inspections in 2002 and 20 in 2003 up to 31 March. The Securities Commission conducted 78 inspections of registrants and licensees from March 2001 to May 2002, and an additional 29 inspections up to 31 March 2003.

56. The Attorney General's Office also established an international co-operation unit, which processed 120 legal assistance requests in 2002 and 35 in 2003 up to 15 May. The FATF will continue to monitor the situation in the Bahamas, particularly in light of continuing concerns expressed by FATF members regarding inadequate international co-operation.

Dominica

57. Dominica was identified as an NCCT in June 2000. After that time, Dominica enacted significant legislative reforms that addressed issues relating to the criminalisation of money laundering,

the establishment of a Money Laundering Supervisory Authority (MLSA) and of a financial intelligence unit, and requirements for record-keeping, reporting of suspicious transactions, and customer identification. The Exchange of Information Act, effective January 31, 2002, expanded Dominica's authority to assist foreign regulatory authorities. Dominica was among the first to place its offshore banks under the direct supervision of the Eastern Caribbean Central Bank (ECCB), in conjunction with the local supervisory authorities. As a result of adequate implementation of these reforms, including significant improvement on international co-operation matters, Dominica was de-listed in October 2002.

58. Since that time, implementation has continued to improve in Dominica. The FIU had received 100 suspicious (69) and large (31) transaction reports as of 31 December 2002 and investigated 65; an additional 8 were received and investigated in 2003 up to 15 May. The FIU co-operates with foreign FIUs and police units; it will become an official Egmont Group member at the July 2003 Egmont Plenary meeting. Dominica has significantly reduced the size of its offshore sector, with only one offshore bank remaining operational. The new Anti-Money Laundering Supervisory Authority inspected 12 scheduled entities between September 2002 and 15 May 2003. To date Dominica had responded to all requests for mutual legal assistance and all requests under the Exchange of Information Act.

Grenada

59. Grenada was placed on the NCCTs list in September 2001. Since that time, Grenada has achieved significant progress, including legislative reforms that permit regulatory access to account records, allow the regulator to communicate relevant information to other Grenadian authorities, and the creation of a registration mechanism for bearer shares of IBCs.

60. Grenada also enacted the Financial Intelligence Unit (FIU) Act (No. 1 of 2003), the Exchange of Information Act (No. 2 of 2003) and the Proceeds of Crime Act on 31 January 2003. An MOU between Grenada and the ECCB now gives the ECCB a supervisory role in the regulation of the offshore banking and trust businesses. By February 2003, the size of the offshore sector had been drastically reduced, with the remaining offshore banks being liquidated or under government oversight. The FIU had a staff of 5 and had received 29 suspicious transaction reports as of December 2002. As a result of implementation of the above measures, and adequate responses to requests for mutual legal assistance, Grenada was de-listed in February 2003.

61. By May 2003, the FIU had received a total of 58 STRs. The FIU was investigating two money laundering cases, with another case proceeding in court. International co-operation has also continued to improve in 2003; Grenada has responded to the two requests from foreign regulators, all three requests for legal assistance, and seven requests from foreign police agencies and FIUs. Grenada should complete the process of amending the Exchange of Information Act 2003 to clarify Grenada's ability to co-operate with foreign regulator authorities and the Offshore Banking Act to provide a statutory role for the ECCB.

Hungary

62. Hungary was identified as an NCCT in June 2001. After that time, Hungary significantly enhanced its anti-money laundering regime. New legislation abolished anonymous passbooks by requiring registration, i.e. the identification of both the depositors and the beneficiaries and the conversion of existing passbooks to registered form. The legislation also extended anti-money laundering controls to non-banking sectors including casinos, real estate agents, and tax consultants. As a result of these reforms and adequate implementation thereof, Hungary was removed from the NCCTs list in June 2002.

63. In July 2002, Hungary began the second phase of the transformation of anonymous accounts, which requires that the data on all the owners of accounts above 8,400 euros are to be reported. 5,809

STRs were reported from January-November 2002, an increase of more than three times for the previous year. An additional 3,193 STRs were received between 1 January and 1 June 2003. Between 1 January and 31 March 2003, more than 90% of the value of anonymous deposits had been registered. Two new investigations had also begun. Co-operation with Hungary also remained good since de-listing. Act XV of 2003, enacted on 18 March 2003 and in force as of 16 June 2003, extends anti-money laundering controls to lawyers and notaries.

64. Hungary has adequately addressed all the previously identified deficiencies and therefore will no longer require monitoring by the FATF. Future monitoring of Hungary will be conducted within the Council of Europe's MONEYVAL and its relevant monitoring mechanisms.

Israel

65. Israel was identified as an NCCT in June 2000. After that time, Israel adopted legislation and regulations for the money laundering criminal offence, customer identification, and record keeping and reporting requirements. In January 2002, the Israel Money Laundering Prohibition Authority (IMPA) was established and functions as an FIU. The FIU was admitted into the Egmont Group in June 2002. After substantial implementation of these reforms, Israel was de-listed in June 2002.

66. After June 2002, the IMPA continued efforts to improve financial institutions' reporting compliance. From February 2002—January 2003 the IMPA received approximately 1,100 STRs; 200 were undergoing further analysis and 81 were disseminated to other agencies. Co-operation with other law enforcement agencies and foreign FIUs also increased; 5 MOUs with foreign FIUs had been finalised and 20 more were under negotiation. During 2002 the IMPA had responded to 12 of the 30 requests for information and was processing the other requests as of February 2003. During 2002 a total of five money laundering cases yielded indictments, one was under consideration of the District prosecutor, one yielded a request for a civil forfeiture, one case ended with the arrest and indictment of suspects in another country, and eleven cases were in various stages of investigation.

67. Israel has also instituted a program for inspecting financial institutions. As of April 2003, the Central Bank had completed comprehensive inspections in three banking corporations (about 40% of banking activity), and plans to complete comprehensive inspections of all five of the largest banking groups in Israel by year's end (95% of banking activity). Customer identification procedures for existing customers of banks and portfolio managers are set to be completed in August 2003. The FATF welcomes Israel's plans to accelerate its compliance monitoring of Israeli banks in order to complete general anti-money laundering examinations in all banks by September 2003. The FATF will continue to monitor the situation in Israel as it continues to implement its banking inspection and customer identification procedures.

Lebanon

68. Lebanon was identified as an NCCT in June 2000. Law No. 318 of 26 April 2001 and Circular No. 83 of 18 May 2001 addressed the criminalisation of money laundering, bank secrecy, customer identification, and suspicious transaction reporting. The law also created the Special Investigation Commission as the FIU. The SIC is an independent entity with judicial status that investigates money laundering operations and monitors compliance of banks and other financial institutions with the provisions of Law No. 318. After adequate implementation, Lebanon was de-listed in June 2002.

69. For 2002, the FIU received 138 STRs, 75 of which came from local reporting and 63 from foreign cases. Twenty-four cases were passed on to the General Prosecutor or to reporting sources, and 11 bank accounts had been frozen. The SIC investigated 103 cases and lifted bank secrecy in 79 of these cases. In the first three months of 2003, the SIC received another 50 STRs, and the General Prosecutor had brought the first two money laundering cases to the Criminal Court.

70. The FATF encourages Lebanon to enact proposed changes to Law No. 318 that could expand the number of money laundering cases brought for prosecution. The FATF will continue to monitor the implementation of Lebanon's anti-money laundering regime, with particular attention paid to general compliance and STR reporting in the banking and non-banking sectors, the number and quality of investigations, seizures, and prosecutions for money laundering offences.

The Marshall Islands

71. After the Republic of the Marshall Islands (RMI) was identified as an NCCT in June 2000, it passed the Banking (Amendment) Act of 2000 (P.L. 2000-20) on 31 October 2000. The Act addresses the following areas: criminalisation of money laundering, customer identification for accounts, and reporting of suspicious transactions. On 27 May 2002, the RMI enacted a set of regulations that provide standards for reporting and compliance. The Marshall Islands had increased the number of IBCs from 3,000 in June 2002 to nearly 8,500 in October 2002, but the arrangements for controlling registrations had improved. The RMI was de-listed in October 2002.

72. The FATF continues to monitor the situation in the Marshall Islands, with particular attention to ensuring that adequate information regarding legal and business entities is recorded and made available to investigators.

Niue

73. After being listed as an NCCT in June 2000, Niue enacted significant reforms to address the deficiencies. The Financial Transactions Reporting Act 2000 addressed requirements dealing with reporting of suspicious transactions, the establishment of an FIU, and partly addressed customer identification. The International Banking Repeal Act 2002, which was brought into force on 5 June 2002, eliminated Niue's offshore banks as of October 2002. Although Niue retained its 5,500 IBCs, company registry information is now maintained in Niue so as to provide local access to current information. As a result of these measures, Niue was de-listed in October 2002.

74. The FATF continues to monitor the situation in Niue, with particular attention to ensuring that adequate information regarding legal and business entities is recorded and made available to investigators.

Russia

75. After being identified as an NCCT in June 2000, Russia has enacted significant reforms to address the issues identified. Federal Law No. 115-FZ "On Combating the Legalisation (Laundering) of Income Obtained by Criminal Means" came into effect 1 February 2002 and included customer identification requirements, a suspicious activity reporting system, procedures for international co-operation, and provisions for a Commission for Financial Monitoring (KFM) to operate as a financial intelligence unit (FIU). The KFM began operations on 1 February 2002 and was admitted into the Egmont Group in June 2002. Russia was de-listed by the FATF in October 2002.

76. After de-listing, Russia continued to implement and enhance its new anti-money laundering structures. Law No. 115-FZ was amended in January 2003 to include measures to address terrorist financing and to expand the scope of the law to include gaming entities, entities involved in the purchase and sale of precious metals and stones, and investment funds. The KFM is also now tasked with supervising entities for anti-money laundering compliance which do not fall under the jurisdiction of an existing supervisory authority, including gambling services, leasing companies, and pawn shops, and the KFM began measures to implement these provisions. As of April 2003, the KFM had received approximately 320,000 mandatory transaction reports and 234,000 suspicious transaction reports, which resulted in 124 cases referred to law enforcement bodies. The KFM had responded to 73 requests from foreign FIUs. The Operational Detection Bureau (OSB), a new specialised anti-money laundering investigation unit within the Ministry of Interior Affairs, had approximately 1,400 open cases.

77. As an observer member to the FATF, Russia also underwent a mutual evaluation in April 2003. A summary of the findings can be found in the FATF Annual Report for 2002-2003 of 20 June 2003.

St. Kitts and Nevis

78. After being placed on the NCCTs list in June 2000, St. Kitts and Nevis enacted comprehensive legislation to address the identified deficiencies. These new measures expanded the money laundering offence, required customer identification and record keeping procedures, and suspicious transaction reporting, and established a financial intelligence unit. New measures also enhanced the licensing, regulation and supervision of offshore entities. A new mechanism to register bearer shares that includes identifying the beneficial owners was instituted. The ECCB now vets offshore bank applications and supervises Nevis' one offshore bank in conjunction with the Nevis regulator. As a result of adequate implementation of these measures, St. Kitts and Nevis was removed from the NCCTs list in June 2002.

79. By January 2003, the FIU had a staff of seven and had received 82 STRs, with 44 referrals to police and 13 investigations on-going. The FIU had responded to 24 of the 40 requests from foreign jurisdictions that it had received. By May 2003 the FIU had received an additional 21 STRs, and had responded to 3 of 16 additional requests from foreign FIUs.

80. Although there is an indirect mechanism for regulatory co-operation between the ECCB and foreign bank regulators, the FATF encourages the efforts of the ECCB and St. Kitts and Nevis to continue with its efforts to establish a direct gateway. St. Kitts and Nevis has adequately addressed all the previously identified deficiencies and therefore will no longer require monitoring by the FATF. Future monitoring of St. Kitts and Nevis will be conducted within the CFATF and its relevant monitoring mechanisms.

IV. CONCLUSIONS AND THE WAY FORWARD

81. The reviews carried out in 2000 and 2001 by the FATF have been extremely productive. Most jurisdictions participated actively and constructively in the reviews. The reviews of jurisdictions against the 25 criteria have revealed – and stimulated – many ongoing efforts by governments to improve their systems. As of June 2003, most jurisdictions had enacted significant reforms and are well on their way towards comprehensive anti-money laundering regimes.

82. Nevertheless, serious systematic problems remain in several jurisdictions. Following the progress made by the jurisdictions deemed to be non-cooperative in June 2000, June 2001, and September 2001, the list of NCCTs now comprises the following jurisdictions:

Cook Islands
Egypt
Guatemala
Indonesia
Myanmar
Nauru
Nigeria
Philippines
Ukraine

83. These jurisdictions are strongly urged to adopt the necessary measures to improve their rules and practices as expeditiously as possible in order to remedy the remaining deficiencies identified in the reviews. Pending adoption and implementation of appropriate legislative and other measures, and in accordance with Recommendation 21, the FATF recommends that financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from the "non-cooperative countries and territories" mentioned in paragraph 82 and in so doing take into account issues raised in the relevant summaries in Section II of this report and any progress made by these jurisdictions since being listed as NCCTs.

84. The FATF notes with concern the failure by the governments of Indonesia and Myanmar to make more substantive progress since June 2002. Although they have enacted some anti-money laundering measures, serious deficiencies remain that will inhibit implementation of comprehensive anti-money laundering systems.

85. Should those countries or territories identified as non-cooperative maintain their detrimental rules and practices despite having been encouraged to make certain reforms, FATF members would need to consider the adoption of counter-measures against such jurisdictions. With respect to those countries listed in June 2000, June 2001 and September 2001, whose progress addressing deficiencies has stalled, the FATF will consider the adoption of additional counter-measures as well.

86. The FATF and its members will continue the dialogue with these jurisdictions. FATF members are also prepared to provide technical assistance, where appropriate, to help jurisdictions in the design and implementation of their anti-money laundering systems.

87. All countries and territories that are part of the global financial system are urged to change any rules or practices which impede the fight against money laundering. To this end, the FATF will continue its work to improve its members' and non-members' implementation of the FATF Forty Recommendations. It will also encourage and support the regional anti-money laundering bodies in their ongoing efforts. In this context, the FATF also calls on all the jurisdictions mentioned in this report to adopt legislation and improve their rules or practices as expeditiously as possible, in order to remedy the deficiencies identified in the reviews.

88. The FATF intends to remain fully engaged with all the jurisdictions identified in paragraph 82. The FATF will continue to place on the agenda of each plenary meeting the issue of non-cooperative countries and territories, to monitor any progress which may materialise, and to revise its findings, including the removal of jurisdictions' names from the list of NCCTs, as warranted.

89. The FATF will continue to monitor weaknesses in the global financial system that could be exploited for money laundering purposes. This could lead to further jurisdictions being examined. Future reports will continue to update the FATF's findings in relation to these matters.

90. The FATF expects that this exercise along with its other anti-money laundering efforts, and the activities of regional anti-money laundering bodies, will provide an ongoing stimulus for all jurisdictions to bring their regimes into compliance with the FATF Forty Recommendations, in the global fight against money laundering.

APPENDIX 1

LIST OF CRITERIA FOR DEFINING NON-COOPERATIVE COUNTRIES OR TERRITORIES[7]

A. Loopholes in financial regulations

(i) No or inadequate regulations and supervision of financial institutions

1. Absence or ineffective regulations and supervision for all financial institutions in a given country or territory, onshore or offshore, on an equivalent basis with respect to international standards applicable to money laundering.

(ii) Inadequate rules for the licensing and creation of financial institutions, including assessing the backgrounds of their managers and beneficial owners

2. Possibility for individuals or legal entities to operate a financial institution without authorisation or registration or with very rudimentary requirements for authorisation or registration.

3. Absence of measures to guard against holding of management functions and control or acquisition of a significant investment in financial institutions by criminals or their confederates.

(iii) Inadequate customer identification requirements for financial institutions

4. Existence of anonymous accounts or accounts in obviously fictitious names.

5. Lack of effective laws, regulations, agreements between supervisory authorities and financial institutions or self-regulatory agreements among financial institutions on identification by the financial institution of the client and beneficial owner of an account:

- no obligation to verify the identity of the client;
- no requirement to identify the beneficial owners where there are doubts as to whether the client is acting on his own behalf;
- no obligation to renew identification of the client or the beneficial owner when doubts appear as to their identity in the course of business relationships;
- no requirement for financial institutions to develop ongoing anti-money laundering training programmes.

6. Lack of a legal or regulatory obligation for financial institutions or agreements between supervisory authorities and financial institutions or self-agreements among financial institutions to record and keep, for a reasonable and sufficient time (five years), documents connected with the identity of their clients, as well as records on national and international transactions.

7. Legal or practical obstacles to access by administrative and judicial authorities to information with respect to the identity of the holders or beneficial owners and information connected with the transactions recorded.

(iv) Excessive secrecy provisions regarding financial institutions

---

[7] This list should be read in conjunction with the attached comments and explanations.

8. Secrecy provisions which can be invoked against, but not lifted by competent administrative authorities in the context of enquiries concerning money laundering.

9. Secrecy provisions which can be invoked against, but not lifted by judicial authorities in criminal investigations related to money laundering.

(v) Lack of efficient suspicious transactions reporting system

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

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

B. Obstacles raised by other regulatory requirements

(i) Inadequate commercial law requirements for registration of business and legal entities

12. Inadequate means for identifying, recording and making available relevant information related to legal and business entities (name, legal form, address, identity of directors, provisions regulating the power to bind the entity).

(ii) Lack of identification of the beneficial owner(s) of legal and business entities

13. Obstacles to identification by financial institutions of the beneficial owner(s) and directors/officers of a company or beneficiaries of legal or business entities.

14. Regulatory or other systems which allow financial institutions to carry out financial business where the beneficial owner(s) of transactions is unknown, or is represented by an intermediary who refuses to divulge that information, without informing the competent authorities.

C. Obstacles to international co-operation

(i) Obstacles to international co-operation by administrative authorities

15. Laws or regulations prohibiting international exchange of information between administrative anti-money laundering authorities or not granting clear gateways or subjecting exchange of information to unduly restrictive conditions.

16. Prohibiting relevant administrative authorities to conduct investigations or enquiries on behalf of, or for account of their foreign counterparts.

17. Obvious unwillingness to respond constructively to requests (e.g. failure to take the appropriate measures in due course, long delays in responding).

18. Restrictive practices in international co-operation against money laundering between supervisory authorities or between FIUs for the analysis and investigation of suspicious transactions, especially on the grounds that such transactions may relate to tax matters.

(ii) Obstacles to international co-operation by judicial authorities

19. Failure to criminalise laundering of the proceeds from serious crimes.

20. Laws or regulations prohibiting international exchange of information between judicial authorities (notably specific reservations to the anti-money laundering provisions of international agreements) or placing highly restrictive conditions on the exchange of information.

21. Obvious unwillingness to respond constructively to mutual legal assistance requests (e.g. failure to take the appropriate measures in due course, long delays in responding).

22. Refusal to provide judicial co-operation in cases involving offences recognised as such by the requested jurisdiction especially on the grounds that tax matters are involved.

D. Inadequate resources for preventing and detecting money laundering activities

(i) Lack of resources in public and private sectors

23. Failure to provide the administrative and judicial authorities with the necessary financial, human or technical resources to exercise their functions or to conduct their investigations.

24. Inadequate or corrupt professional staff in either governmental, judicial or supervisory authorities or among those responsible for anti-money laundering compliance in the financial services industry.

(ii) Absence of a financial intelligence unit or of an equivalent mechanism

25. Lack of a centralised unit (i.e., a financial intelligence unit) or of an equivalent mechanism for the collection, analysis and dissemination of suspicious transactions information to competent authorities.

CRITERIA DEFINING NON-COOPERATIVE COUNTRIES OR TERRITORIES

1. International co-operation in the fight against money laundering not only runs into direct legal or practical impediments to co-operation but also indirect ones. The latter, which are probably more numerous, include obstacles designed to restrict the supervisory and investigative powers of the relevant administrative[8] or judicial authorities[9] or the means to exercise these powers. They deprive the State of which legal assistance is requested of the relevant information and so prevent it from responding positively to international co-operation requests.

2. This document identifies the detrimental rules and practices which obstruct international co-operation against money laundering. These naturally affect domestic prevention or detection of money laundering, government supervision and the success of investigations into money laundering. Deficiencies in existing rules and practices identified herein have potentially negative consequences for the quality of the international co-operation which countries are able to provide.

3. The detrimental rules and practices which enable criminals and money launderers to escape the effect of anti-money laundering measures can be found in the following areas:

- the financial regulations, especially those related to identification;
- other regulatory requirements;
- the rules regarding international administrative and judicial co-operation; and
- the resources for preventing, detecting and repressing money laundering.

A. Loopholes in financial regulations

(i) No or inadequate regulations and supervision of financial institutions (Recommendation 26)

4. All financial systems should be adequately regulated and supervised. Supervision of financial institutions is essential, not only with regard to purely prudential aspects of financial regulations, but also with regard to implementing anti-money laundering controls. Absence or ineffective regulations and supervision for all financial institutions in a given country or territory, offshore or onshore, on an equivalent basis with respect to international standards applicable to money laundering is a detrimental practice.[10]

(ii) Inadequate rules for the licensing and creation of financial institutions, including assessing the backgrounds of their managers and beneficial owners (Recommendation 29)

5. The conditions surrounding the creation and licensing of financial institutions in general and banks in particular create a problem upstream from the central issue of financial secrecy. In addition to the rapid increase of insufficiently regulated jurisdictions and offshore financial centres, we are witnessing a proliferation in the number of financial institutions in such jurisdictions. They are easy to set up, and the identity and background of their founders, managers and beneficial owners are frequently not,

---

8 The term "administrative authorities " is used in this document to cover both financial regulatory authorities and certain financial intelligence units (FIUs).

9 The term "judicial authorities" is used in this document to cover law enforcement, judicial/prosecutorial authorities, authorities which deal with mutual legal assistance requests, as well as certain types of FIUs.

10 For instance, those established by the Basle Committee on Banking Supervision, the International Organisation of Securities Commissions, the International Association of Insurance Supervisors, the International Accounting Standards Committee and the FATF.

or insufficiently, checked. This raises a potential danger of financial institutions (banks and non-bank financial institutions) being taken over by criminal organisations, whether at start-up or subsequently.

6. The following should therefore be considered as detrimental:

- possibility for individuals or legal entities to operate a financial institution[11] without authorisation or registration or with very rudimentary requirements for authorisation or registration; and,

- absence of measures to guard against the holding of management functions, the control or acquisition of a significant investment in financial institutions by criminals or their confederates (Recommendation 29).

(iii) Inadequate customer identification requirements for financial institutions

7. FATF Recommendations 10, 11 and 12 call upon financial institutions not to be satisfied with vague information about the identity of clients for whom they carry out transactions, but should attempt to determine the beneficial owner(s) of the accounts kept by them. This information should be immediately available for the administrative financial regulatory authorities and in any event for the judicial and law enforcement authorities. As with all due diligence requirements, the competent supervisory authority should be in a position to verify compliance with this essential obligation.

8. Accordingly, the following are detrimental practices:

- the existence of anonymous accounts or accounts in obviously fictitious names, i.e. accounts for which the customer and/or the beneficial owner have not been identified (Recommendation 10);

- lack of effective laws, regulations or agreements between supervisory authorities and financial institutions or self-regulatory agreements among financial institutions[12] on identification[13] by the financial institution of the client, either occasional or usual, and the beneficial owner of an account when a client does not seem to act in his own name (Recommendations 10 and 11), whether an individual or a legal entity (name and address for individuals; type of structure, name of the managers and commitment rules for legal entities...);

- lack of a legal or regulatory obligation for financial institutions to record and keep, for a reasonable and sufficient time (at least five years), documents connected with the identity of their clients (Recommendation 12), e.g. documents certifying the identity and legal structure of the legal entity, the identity of its managers, the beneficial owner and any record of changes in or transfer of ownership as well as records on domestic and international transactions (amounts, type of currency);

---

[11] The Interpretative Note to bureaux de change states that the minimum requirement is for there to be "an effective system whereby the bureaux de change are known or declared to the relevant authorities".

[12] The agreements and self-regulatory agreements should be subject to strict control.

[13] No obligation to verify the identity of the account-holder; no requirement to identify the beneficial owners when the identification of the account-holder is not sufficiently established; no obligation to renew identification of the account-holder or the beneficial owner when doubts appear as to their identity in the course of business relationships; no requirement for financial institutions to develop ongoing anti-money laundering training programmes.

- legal or practical obstacles to access by the administrative and judicial authorities to information with respect to the identity of the holders or beneficiaries of an account at a financial institution and to information connected with the transactions recorded (Recommendation 12).

(iv) Excessive secrecy provisions regarding financial institutions

9. Countries and territories offering broad banking secrecy have proliferated in recent years. The rules for professional secrecy, like banking secrecy, can be based on valid grounds, i.e., the need to protect privacy and business secrets from commercial rivals and other potentially interested economic players. However, as stated in Recommendations 2 and 37, these rules should nevertheless not be permitted to pre-empt the supervisory responsibilities and investigative powers of the administrative and judicial authorities in their fight against money laundering. Countries and jurisdictions with secrecy provisions must allow for them to be lifted in order to co-operate in efforts (foreign and domestic) to combat money laundering.

10. Accordingly, the following are detrimental:

- secrecy provisions related to financial activities and professions, notably banking secrecy, which can be invoked against, but not lifted by competent administrative authorities in the context of enquiries concerning money laundering;

- secrecy provisions related to financial activities and professions, specifically banking secrecy, which can be invoked against, but not lifted by judicial authorities in criminal investigations relating to money laundering.

(v) Lack of efficient suspicious transaction reporting system

11. A basic rule of any effective anti-money laundering system is that the financial sector must help to detect suspicious transactions. The forty Recommendations clearly state that financial institutions should report their "suspicions" to the competent authorities (Recommendation 15). In the course of the mutual evaluation procedure, systems for reporting unusual transactions have been assessed as being in conformity with the Recommendations. Therefore, for the purpose of the exercise on non-cooperative jurisdictions, in the event that a country or territory has established a system for reporting unusual transactions instead of suspicious transactions (as mentioned in the forty Recommendations), it should not be treated as non-cooperative on this basis, provided that such a system requires the reporting of all suspicious transactions.

12. The absence of an efficient mandatory system for reporting suspicious or unusual transactions to a competent authority, provided that such a system aims to detect and prosecute money laundering, is a detrimental rule. The reports should not be drawn to the attention of the customers (Recommendation 17) and the reporting parties should be protected from civil or criminal liability (Recommendation 16).

13. It is also damaging if the competent authority does not monitor whether financial institutions comply with their reporting obligations, and if there is a lack of criminal or administrative sanctions for financial institutions in respect to the obligation to report suspicious or unusual transactions.

B. Impediments set by other regulatory requirements

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

is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering.

(i) Inadequate commercial law requirements for registration of business and legal entities

15. Inadequate means for identifying, recording and making available relevant information related to legal and business entities (identity of directors, provisions regulating the power to bind the entity, etc.), has detrimental consequences at several levels:

- it may significantly limit the scope of information immediately available for financial institutions to identify those of their clients who are legal structures and entities, and it also limits the information available to the administrative and judicial authorities to conduct their enquiries;

- as a result, it may significantly restrict the capacity of financial institutions to exercise their vigilance (especially relating to customer identification) and may limit the information that can be provided for international co-operation.

(ii) Lack of identification of the beneficial owner(s) of legal and business entities (Recommendations 9 and 25)

16. Obstacles to identification by financial institutions of the beneficial owner(s) and directors/officers of a company or beneficiaries of legal or business entities are particularly detrimental practices: this includes all types of legal entities whose beneficial owner(s), managers cannot be identified. The information regarding the beneficiaries should be recorded and updated by financial institutions and be available for the financial regulatory bodies and for the judicial authorities.

17. Regulatory or other systems which allow financial institutions to carry out financial business where the beneficial owner(s) of transactions is unknown, or is represented by an intermediary who refuses to divulge that information, without informing the competent authorities, should be considered as detrimental practices.

C. Obstacles to international co-operation

(i) At the administrative level

18. Every country with a large and open financial centre should have established administrative authorities to oversee financial activities in each sector as well as an authority charged with receiving and analysing suspicious transaction reports. This is not only necessary for domestic anti-money laundering policy; it also provides the necessary foundations for adequate participation in international co-operation in the fight against money laundering.

19. When the aforementioned administrative authorities in a given jurisdiction have information that is officially requested by another jurisdiction, the former should be in a position to exchange such information promptly, without unduly restrictive conditions (Recommendation 32). Legitimate restrictions on transmission of information should be limited, for instance, to the following:

- the requesting authority should perform similar functions to the authority to which the request is addressed;

- the purpose and scope of information to be used should be expounded by the requesting authority, the information transmitted should be treated according to the scope of the request;

- the requesting authority should be subject to a similar obligation of professional or official secrecy as the authority to which the request is addressed;

- exchange of information should be reciprocal.

In all events, no restrictions should be applied in a bad faith manner.

20. In light of these principles, laws or regulations prohibiting international exchange of information between administrative authorities or not granting clear gateways or subjecting this exchange to highly restrictive conditions should be considered abusive. In addition, laws or regulations that prohibit the relevant administrative authorities from conducting investigations or enquiries on behalf of, or for account of their foreign counterparts when requested to do so can be a detrimental practice.

21. Obvious unwillingness to respond constructively to requests (e.g. failure to take the appropriate measures in due course, long delays in responding) is also a detrimental practice.

22. Restrictive practices in international co-operation against money laundering between supervisory authorities or between FIUs for the analysis and investigation of suspicious transactions, especially on the grounds that such transactions may relate to tax matters (fiscal excuse[14]). Refusal only on this basis is a detrimental practice for international co-operation against money laundering.

(ii) At the judicial level

23. Criminalisation of money laundering is the cornerstone of anti-money laundering policy. It is also the indispensable basis for participation in international judicial co-operation in this area. Hence, failure to criminalise laundering of the proceeds from serious crimes (Recommendation 4) is a serious obstacle to international co-operation in the international fight against money laundering and therefore a very detrimental practice. As stated in Recommendation 4, each country would determine which serious crimes would be designated as money laundering predicate offences.

24. Mutual legal assistance (Recommendations 36 to 40) should be granted as promptly and completely as possible if formally requested. Laws or regulations prohibiting international exchange of information between judicial authorities (notably specific reservations formulated to the anti-money laundering provisions of mutual legal assistance treaties or provisions by countries that have signed a multilateral agreement) or placing highly restrictive conditions on the exchange of information are detrimental rules.

25. Obvious unwillingness to respond constructively to mutual legal assistance requests (e.g. failure to take the appropriate measures in due course, long delays in responding) is also a detrimental practice.

26. The presence of tax evasion data in a money laundering case under judicial investigation should not prompt a country from which information is requested to refuse to co-operate. Refusal to provide judicial co-operation in cases involving offences recognised as such by the requested jurisdiction, especially on the grounds that tax matters are involved is a detrimental practice for international co-operation against money laundering.

D. Inadequate resources for preventing, detecting and repressing money laundering activities

(i) Lack of resources in public and private sectors

[14] "Fiscal excuse" as referred to in the Interpretative Note to Recommendation 15.

27. Another detrimental practice is failure to provide the administrative and judicial authorities with the necessary financial, human or technical resources to ensure adequate oversight and to conduct investigations. This lack of resources will have direct and certainly damaging consequences for the ability of such authorities to provide assistance or take part in international co-operation effectively.

28. The detrimental practices related to resource constraints that result in inadequate or corrupt professional staff should not only concern governmental, judicial or supervisory authorities but also the staff responsible for anti-money laundering compliance in the financial services industry.

(ii) Absence of a financial intelligence unit or of an equivalent mechanism

29. In addition to the existence of a system for reporting suspicious transactions, a centralised governmental authority specifically dealing with anti-money laundering controls and/or the enforcement of measures in place must exist. Therefore, lack of centralised unit (i.e., a financial intelligence unit) or of an equivalent mechanism for the collection, analysis and dissemination of suspicious transactions information to competent authorities is a detrimental rule.

APPENDIX 2

FATF'S POLICY CONCERNING IMPLEMENTATION AND DE-LISTING IN RELATION TO NCCTs

The FATF has articulated the steps that need to be taken by Non-Cooperative Countries or Territories (NCCTs) in order to be removed from the NCCT list. These steps have focused on what precisely should be required by way of implementation of legislative and regulatory reforms made by NCCTs to respond to the deficiencies identified by the FATF in the NCCT reports. This policy concerning implementation and de-listing enables the FATF to achieve equal and objective treatment among NCCT jurisdictions.

In order to be removed from the NCCT list:

1. An NCCT must enact laws and promulgate regulations that comply with international standards to address the deficiencies identified by the NCCT report that formed the basis of the FATF's decision to place the jurisdiction on the NCCT list in the first instance.

2. The NCCTs that have made substantial reform in their legislation should be requested to submit to the FATF through the applicable regional review group, an implementation plan with targets, milestones, and time frames that will ensure effective implementation of the legislative and regulatory reforms. The NCCT should be asked particularly to address the following important determinants in the FATF's judgement as to whether it can be de-listed: filing of suspicious activity reports; analysis and follow-up of reports; the conduct of money laundering investigations; examinations of financial institutions (particularly with respect to customer identification); international exchange of information; and the provision of budgetary and human resources.

3. The appropriate regional review groups should examine the implementation plans submitted and prepare a response for submission to the NCCT at an appropriate time. The Chairs of the four review groups (Americas; Asia/Pacific; Europe; Africa and the Middle East) should report regularly on the progress of their work. A meeting of those Chairs, if necessary, to keep consistency among their responses to the NCCTs.

4. The FATF, on the initiative of the applicable review group chair or any member of the review group, should make an on-site visit to the NCCT at an appropriate time to confirm effective implementation of the reforms.

5. The review group chair shall report progress at subsequent meetings of the FATF. When the review groups are satisfied that the NCCT has taken sufficient steps to ensure continued effective implementation of the reforms, they shall recommend to the Plenary the removal of the jurisdiction from the NCCT list. Based on an overall assessment encompassing the determinants in paragraph 2, the FATF will rely on its collective judgement in taking the decision.

6. Any decision to remove countries from the list should be accompanied by a letter from the FATF President:

   (a) clarifying that de-listing does not indicate a perfect anti-money laundering system;

   (b) setting out any outstanding concerns regarding the jurisdiction in question;

   (c) proposing a monitoring mechanism to be carried out by FATF in consultation with the relevant FATF-style regional body, which would include the submission of regular implementation reports to the relevant review group and a follow-up visit to assess progress in implementing reforms and to ensure that stated goals have, in fact, been fully achieved.

7. Any outstanding concerns and the need for monitoring the full implementation of legal reforms should also be mentioned in the NCCT public report.

OUTLINE FOR MONITORING PROGRESS OF IMPLEMENTATION

SUBSTANCE

The FATF will monitor progress of de-listed jurisdictions against the implementation plans, specific issues raised in the 2001 progress reports (*e.g.*, phasing out of unidentified accounts) and the experience of FATF members. Subjects addressed may include, as appropriate:

- the issuance of secondary legislation and regulatory guidance;
- inspections of financial institutions planned and conducted;
- STRs systems;
- process for money laundering investigations and prosecutions conducted;
- regulatory, FIU and judicial co-operation;
- adequacy of resources;
- assessment of compliance culture in the relevant sectors.

Financial Action Task Force
on Money Laundering
Groupe d'action financière
sur le blanchiment de capitaux

THE FORTY RECOMMENDATIONS

20 June 2003

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

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

are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisonal measures and confiscation

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

[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.

c) Take reasonable measures to establish the source of wealth and source of funds.
d) Conduct enhanced ongoing monitoring of the business relationship.

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

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

8. Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with 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/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15,000.

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

Recommendation 5

Customer due diligence and tipping off

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

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

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

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

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

CDD for legal persons and arrangements

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

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

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

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

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

Reliance on identification and verification already performed

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

Timing of verification

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

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

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

Requirement to identify existing customers

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

Simplified or reduced CDD measures

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

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

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

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

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

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

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

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

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

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

Recommendation 6

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

Recommendation 9

This Recommendation does not apply to outsourcing or agency relationships.

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

Recommendations 10 and 11

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

Recommendation 13

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

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

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

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

Recommendation 14 (tipping off)

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

Recommendation 15

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

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

Recommendation 16

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

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

Recommendation 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.