



ASIA/PACIFIC GROUP ON MONEY
LAUNDERING



Mutual Evaluation Report

Anti-Money Laundering and Combating the
Financing of Terrorism

India

25 June 2010

India is a member of the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG). This joint APG-FATF evaluation was adopted by the FATF Plenary on 25 June 2010 and was also adopted at the APG Plenary on 15 July 2010.

© 2010 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Requests for permission to further disseminate, reproduce or translate all or part of this publication should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

TABLE OF CONTENTS

| | |
|--|-----|
| PREFACE | 5 |
| 1. GENERAL..... | 6 |
| 2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES | 36 |
| 2.1 Criminalisation of Money Laundering (R.1 & 2)..... | 36 |
| 2.2 Criminalisation of Terrorist Financing (SR.II)..... | 45 |
| 2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)..... | 54 |
| 2.4 Freezing of funds used for terrorist financing (SR.III) | 62 |
| 2.5 The Financial Intelligence Unit and its functions (R.26)..... | 68 |
| 2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R. 27 & 28) | 77 |
| 2.7 Cross Border Declaration or Disclosure (SR.IX) | 84 |
| 3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS..... | 92 |
| 3.1 Risk of money laundering or terrorist financing | 98 |
| 3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)..... | 98 |
| 3.3 Third parties and introduced business (R.9)..... | 118 |
| 3.4 Financial institution secrecy or confidentiality (R.4) | 119 |
| 3.5 Record-keeping and wire transfer rules (R.10 & SR.VII) | 120 |
| 3.6 Monitoring of transactions and relationships (R.11 & 21)..... | 132 |
| 3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)..... | 137 |
| 3.8 Internal controls, compliance, audit and foreign Branches (R.15 & 22) | 150 |
| 3.9 Shell banks (R.18) | 157 |
| 3.10 The supervisory and oversight system - competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)..... | 158 |
| 3.11 Money or value transfer services (SR.VI) | 193 |
| 4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS | 196 |
| 4.1 Customer due diligence and record-keeping (R.12) (applying R.5, 6, and 8 to 11) | 197 |
| 4.2 Suspicious transaction reporting (R.16) (applying R.13 to 15 & 21) | 200 |
| 4.3 Regulation, supervision and monitoring (R.24-25)..... | 201 |
| 4.4 Other non-financial businesses and professions | 204 |
| 5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS | 205 |
| 5.1 Legal Persons – Access to beneficial ownership and control information (R.33) | 205 |
| 5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34) | 210 |
| 5.3 Non-profit organisations (SR.VIII) | 214 |

| | | |
|-----|---|-----|
| 6. | NATIONAL AND INTERNATIONAL CO-OPERATION | 219 |
| 6.1 | <i>National co-operation and co-ordination (R.31)</i> | 219 |
| 6.2 | <i>The Conventions and UN Special Resolutions (R.35 & SR.I)</i> | 223 |
| 6.3 | <i>Mutual Legal Assistance (R.36-38, SR.V)</i> | 225 |
| 6.4 | <i>Extradition (R.37, 39, SR.V)</i> | 233 |
| 6.5 | <i>Other Forms of International Co-operation (R.40 & SR.V)</i> | 236 |
| 7. | OTHER ISSUES | 242 |
| 7.1 | <i>Resources and statistics</i> | 242 |
| 7.2 | <i>Other Relevant AML/CFT Measures or Issues</i> | 242 |
| 7.3 | <i>General framework for AML/CFT system (see also section 1.1)</i> | 242 |
| | TABLES | 243 |

PREFACE

INFORMATION AND METHODOLOGY USED FOR THE EVALUATION OF INDIA

The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of India was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004¹. The evaluation was based on the laws, regulations and other materials supplied by India, and information obtained by the evaluation team during its on-site visit to India from 30 November – 12 December 2009, and subsequently. During the on-site the evaluation team met with officials and representatives of all relevant Indian government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the mutual evaluation report.

The evaluation was conducted by an assessment team, which consisted of FATF and APG experts in criminal law, law enforcement and regulatory issues and members of the FATF and APG Secretariats: Mr. Boudewijn Verhelst, Deputy Attorney General, Deputy Director of the Belgian FIU (CTIF-CFI), Belgium (legal expert); Mr. Anders Cedhagen, Judge of Appeal at the Administrative Court of Appeal in Gothenburg, Sweden (legal expert); Mr. Bill Peoples, Manager International Criminal Law, Ministry of Justice, New Zealand (law enforcement expert); Mr. Richard Chalmers, Adviser, International Division, Financial Services Authority, United Kingdom (financial expert); Ms. Raadhika Sihin, Director, Financial Integrity, National Treasury, Republic of South Africa; Ms. Anne Shere Wallwork, Senior Counselor for Asia, U.S. Department of the Treasury, Office of Terrorist Financing and Financial Crimes, United States (financial expert); Mr. Rick McDonell and Ms. Lia Umans from the FATF Secretariat; and Mr. Gordon Hook from the APG Secretariat. The experts reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.

This report provides a summary of the AML/CFT measures in place in India as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out India's levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

¹ As updated in February 2009.

1. GENERAL

1.1 *General information on India*

Overview

1. India covers an area of 3.29 million square kilometres with a population of 1.17 billion (estimate for July 2009), making it the second most populous country in the world. It is a multilingual society with 22 principal languages. Hindi is the official language and primary tongue of a large percentage of people (38%), while English is commonly used both in personal and business communication. The majority of Indians are Hindus (81.3%), though a significant number are Muslims (12%), Christians (2.3%), Sikhs (1.9%) and others (2.5%, including Buddhists). All Indian citizens over 18 years of age have the right to vote and can contest elections for the National or State Assembly once over the age of 25, however, for the Rajya Sabha (upper house of the Parliament), the minimum age limit to contest elections is 35 years. India shares its political borders with Pakistan and Afghanistan on the west; Bangladesh and Myanmar in the east; and Nepal, China, and Bhutan in the north.

2. India has a federal system consisting of the Union or Central Government, and the State Governments. The 1950 Constitution provides for a parliamentary system of government with a bicameral parliament and three branches: the executive, legislative and judiciary. There are also elected Governments in the 28 States and in the 7 Union Territories. India's parliamentary democracy is the largest in the world.

Economy

3. India has made steady and gradual economic growth after it became independent in 1947. India's diverse economy encompasses traditional village farming, modern agriculture, handicrafts, a wide range of modern industries, and a multitude of services. Services are the major source of economic growth, even though more than half of the workforce is involved in agriculture. Government control over foreign trade and investment has been reduced in many areas. Disinvestment of government shareholding in companies is underway in certain sectors. The economy has known an annual average growth rate of 8.8% in the five financial years² 2003-2004 to 2007-2008. Despite the global economic slowdown, India's economy continued to grow at 6.7% in 2008-2009.

4. India is continuing to move forward with market-oriented economic reforms that began in 1991. Recent reforms include liberalised foreign investment and exchange regimes, industrial decontrol, significant reductions in tariffs and other trade barriers, reform and modernisation of the financial sector, significant adjustments in government monetary and fiscal policies and safeguarding intellectual property rights.

5. The structure of the Indian economy has undergone considerable change in the last decade. This includes the increasing importance of external trade and external capital flows. The rapid growth of the economy from 2003-2004 to 2007-2008 has also made India an attractive destination for foreign capital inflows with net capital inflows increasing from 1.9% of GDP in 2000-2001 to 9.2% in 2007-2008. The services sector has become a major part of the economy with a GDP share of over 50% and the country

² From 1 April in one year until 31 March the following year.

becoming an important hub for exporting IT and IT enabled services. The GDP share of merchandise trade increased from 23.7% in 2003-2004 to over 35% in 2007-2008. Another important feature of India's economy has been the high degree of external dependence on imported energy sources, especially crude oil with the share of imported crude oil in domestic consumption exceeding 75%.

System of Government

Legislative system

6. The division of powers between the Union and the States are listed in a Schedule to the Indian Constitution. The Constitution contains three lists – the Union list, the State list and the concurrent list, which enumerate the subject matters to be dealt by the Centre, States and concurrently between the Centre and the States. If a power is listed as concurrent, the States are prevented from enacting laws that are inconsistent with Union laws. Any residual powers rest with the Union. Currency, banking and external affairs are Union powers, and therefore, money laundering and terrorist financing rest with the Central Government.

7. The Government exercises its broad administrative powers in the name of the President, whose duties are largely ceremonial. A special electoral college indirectly elects the President and the Vice-President for 5-year terms. Their terms are staggered, and the Vice-President does not automatically become President following the death or removal from office of the President.

8. Parliament is the supreme legislative body of India. The Indian parliament comprises the President and the two houses: Lok Sabha (*i.e.* the lower house or the House of Commons) and Rajya Sabha (*i.e.* the upper house or the Council of States). Rajya Sabha is a permanent body and is not subject to dissolution. The Lok Sabha is composed of representatives chosen by direct election.

9. The primary functions of the legislature include overseeing government administration, passing the budget, ventilation of public grievances, and reviewing various subjects, such as development plans, international relations, and national policies. All legislation requires the consent of both Houses of parliament. In the case of financial and related legislation, the will of the Lok Sabha prevails. Finally, the parliament is also vested with the power to initiate amendments to the Constitution.

10. The national executive power is centred in the Council of Ministers (Cabinet), led by the Prime Minister. The President appoints the Prime Minister, who is nominated by legislators of the political party or coalition commanding a parliamentary majority in the Lok Sabha. The President then appoints subordinate Ministers on the advice of the Prime Minister.

11. At the State level, some of the legislatures are bicameral, patterned after the two Houses of the national parliament, however, some States have opted for a unicameral legislature body known as the Legislative Assembly. The States' Chief Ministers are responsible to the legislatures in the same way as the Prime Minister is responsible to parliament. Each State also has a Governor appointed by the President, who may assume certain broad powers when directed by the Central Government. The Central Government exerts greater control over the Union Territories than over the States, although some Territories have gained power to administer their own affairs. Some States are trying to revitalise the traditional village councils, or panchayats, to promote popular democratic participation at the village level, where an important portion of the population still lives.

Judicial system

12. India has a common law legal system. The judiciary's function is to administer justice independently. The judiciary comprises the Supreme Court, the High Courts (the Courts of Appeal), the Subordinate Courts, the Appellate Tribunals, and the Tribunals. The highest court is the Supreme Court of

India, which hears both civil and criminal appeals from the High Courts and the Subordinate Courts. Decisions of the Court of Appeal are binding on lower courts. There are 18 High Courts in the country and three of them have jurisdiction over more than one State. Among the Union Territories, only Delhi has a High Court of its own. One of the unique features of the Indian Constitution is that, notwithstanding the adoption of a federal system and existence of Central Acts and State Acts in their respective spheres, it has generally provided for a single integrated system of courts to administer both Union and State laws.

Source of law and hierarchy of laws

13. The source of law in India is the Constitution, which gives due recognition to codified Central and State Laws. Rules, Regulations, Orders, Declarations, Notifications, and Guidelines are issued under the authority of the respective parent Act and provide greater detail with regard to the statutory obligations. Rules, Regulations, and Orders are published in the government Gazette of India and have the force of law. Laws issued by parliament extend throughout the territory of India and those made by State legislatures apply only within the territory of the State concerned.

Transparency, good governance, ethics and measures against corruption

14. India has signed the United Nations Convention against Corruption (the Merida Convention) on 9 December 2005. Corruption is one of the predicate offences for money laundering. The Government of India has taken steps at both the policy and law enforcement level to limit corruption. To that end, India has established a high-level Central Vigilance Commission (CVC), an independent statutory body responsible for laying down strict vigilance norms, which issues guidelines and conducts inquiries in this regard. In principle, the jurisdiction of the CVC extends to all the organisations to which the executive power of the Union Government extends. The CVC reports to the President through the parliament. Section 8(1)(d) of the Central Vigilance Commission Act, 2003 (CVC Act) restricts its jurisdiction to Group 'A' level officers and other levels of officers as may be notified by the Central Government. The Commission, however, retains its residuary powers to inquire into any individual case in respect of any other employee. Each organisation under the advisory jurisdiction of the CVC has a vigilance unit headed by a Chief Vigilance Officer (CVO). The CVOs act as the extended arms of the CVC and represent the CVC in respect of vigilance matters, particularly, with regard to junior officers who fall outside the jurisdiction of the CVC. The criminal sanctions for corruption (embezzlement and bribery) can be found in the Prevention of Corruption Act, 1988 and the Indian Penal Code, 1860 and range from confiscation of property (which is considered a fine) to fixed-term to life imprisonment.

15. Civil servants in India mainly comprise officers from All India Services (such as the Indian Administrative Services, the Indian Police Services, the Central Civil Services, etc.). They are subject to disciplinary and conduct rules and governed by All Indian Services (Conditions of Service-Residuary Matters) Rules, 1960 and Central Civil Services (Conduct) Rules, 1964. Moreover, these officers are expected to maintain confidentiality and secrecy under the provisions of the Official Secrets Act, 1923.

1.2 *General Situation of Money Laundering and Financing of Terrorism*

16. The following table provides a snapshot of India's general crime situation and gives an indication of the measures India has taken to control it.

Table: Major Indian Penal Code (IPC) Crimes in year 2007

| | Categories of Crime | Number of cases reported | Charge sheeting rate | Conviction rate |
|---|--|--------------------------|----------------------|-----------------|
| A. Violent Crime | | | | |
| 1 | Murder | 32 318 | 83.8 | 35.5 |
| 2 | Attempt to Commit Murder | 27 401 | 88.9 | 31.2 |
| 3 | Culpable Homicide not amounting to murder | 3 644 | 87.1 | 34.2 |
| 4 | Rape | 20 737 | 94.6 | 26.4 |
| 5 | Kidnapping & Abduction | 27 561 | 76.2 | 25.0 |
| 6 | Dacoity | 4 579 | 69.1 | 23.4 |
| 7 | Preparation & Assembly for Dacoity | 3 205 | 98.4 | 25.9 |
| 8 | Robbery | 19 136 | 67.0 | 29.3 |
| 9 | Riots | 59 915 | 90.5 | 19.1 |
| 10 | Arson | 9 024 | 69.2 | 20.4 |
| | Total Violent Crime | 207 520 | 83.9 | 26.4 |
| B. Crime Against Women (IPC+SLL) | | | | |
| 1 | Girls | 20 416 | 77.0 | 25.2 |
| 2 | Molestation | 38 734 | 96.4 | 29.0 |
| 3 | Sexual Harassment | 10 950 | 97.3 | 49.9 |
| 4 | Cruelty by Husband and Relatives | 75 930 | 93.9 | 20.9 |
| 5 | Importation of Girls | 61 | 92.1 | 11.9 |
| | Total Crime Against Women (IPC+SLL) | 146 091 | 91.3 | 27.3 |
| C. Economic Crimes | | | | |
| 1 | Criminal Breach of Trust | 15 531 | 72.3 | 27.2 |
| 2 | Cheating | 65 326 | 74.1 | 24.8 |
| 3 | Counterfeiting | 2 204 | 48.9 | 31.2 |
| 4 | Total Economic Crimes | 83 061 | 72.9 | 25.6 |
| D. Property Crimes | | | | |
| | Burglary | 91 218 | 40.8 | 36.4 |
| 2 | Theft | 285 043 | 42.2 | 40.5 |
| 3 | Total Property Crimes | 376 261 | 41.8 | 39.4 |
| E. Total Crime Against Children | | | | |
| | | 20 410 | 85.8 | 36.6 |
| Total Cognisable Crimes Under IPC | | 1 989 673 | 80.1 | 42.3 |
| Total Cognisable Crimes Under SLL | | 3 743 734 | 95.8 | 83.8 |
| Total Cognisable Crime Under IPC+SLL | | 5 733 407 | 90.6 | 73.9 |

IPC= Indian Penal Code; SLL = Special and Local Laws, CH= Culpable Homicide

17. India itself has identified the major threats as follows:

- a. terrorism and financing of terrorism;
- b. drug trafficking;
- c. counterfeiting of currency;
- d. transnational crime.

Money Laundering

18. As a leader among the emerging economies in Asia with a strongly growing economy and demography, India faces a range of money laundering and terrorist financing risks. The main sources of money laundering in India result from a range of illegal activities committed within and outside the country, mainly drug trafficking; fraud, including counterfeiting of Indian currency; transnational organised crime; human trafficking; and corruption.

19. India is a drug-transit country due to its strategic location between the countries of the Golden Triangle and the Golden Crescent. India is the world's largest producer of licit opium gum for the pharmaceutical preparations but it is estimated that between 20 to 30%³ of the opium crop is diverted. The illicit cultivation is mainly located in the areas of Arunachal Pradesh and Himachal Pradesh in the North of India.

20. According to the Indian authorities, the drug situation in India is a complex combination of many factors as summarised below:

- a. diversion of opium from licit cultivation and indigenous production of low quality heroin;
- b. trafficking of heroin from South West and South East Asia to India and again to Sri Lanka, Maldives and Western countries;
- c. trafficking in hashish from Nepal and further to Europe (hash-tourism);
- d. illicit cultivation of cannabis and opium;
- e. clandestine manufacture of methaqualone and trafficking to South Africa;
- f. diversion of precursor chemicals and other controlled substances;
- g. attempts to establish methamphetamine laboratories in active collaboration with drug operatives based in China; Hong Kong, China; and Canada;
- h. diversion of pharmaceutical preparations and prescription drugs containing psychotropic substances and trafficking to neighbouring countries;
- i. internet pharmacies and misuse of courier services;
- j. involvement of foreign nationals in trafficking and distribution networks, such as Nigerian nationals in case of heroin and Israeli nationals in case of hashish.

21. An area of recent concern has been the diversion of Ketamine (and anaesthetic) from India for abusive purposes. Although there have been no reports of its abuse in India, attempts were made to smuggle Ketamine to certain destinations in South East Asia.

22. Economic crimes involving criminal conspiracy; cheating; criminal breach of trust; forgery of valuable security; will; using as genuine forged documents or electronic records and other crimes of forgery are manifestations of frauds. These criminal activities are amongst the major sources of money laundering, as identified by the law enforcement agencies in India. The Directorate of Enforcement (ED) has been investigating various money laundering cases emanating from these offences. The cases investigated were related to the following offences: corporate frauds; forgery of documents for wrongful acquisition of assets, both moveable and immovable; and counterfeit currency.

23. Counterfeiting of money is highly developed in India. The Indian authorities report that high quality counterfeit Indian currency notes are being printed in Pakistan and are smuggled through transit

³ International Narcotics Control Strategy Report of 2007 Southwest Asia - Section India - Volume I.

nodes in third countries. The authorities are very concerned about the threat it represents for the Indian economy. In a press release issued on 11 August 2009, the Reserve Bank of India (RBI) recognised a sharp increase in the number of fake bank notes detected. The absolute number of counterfeit notes detected at bank branches and the Reserve Bank offices increased from 102 687 in 2000-2001 to 398 111 in 2008-2009. According to the Indian law enforcement agencies, fake notes thus principally originate from Pakistan, but are smuggled through various routes. The most popular among them are via the United Arab Emirates, Nepal and Bangladesh. Fake notes from Dubai are transported by air with the help of bona fide passengers or couriers. Thailand, Malaysia, Myanmar and Sri Lanka are also used as transit points. International airports in Bangalore, Chennai, Calicut, Cochin, Hyderabad, Mangalore, Mumbai and New Delhi are identified as the main landing points. Open land borders with Nepal and porous land borders with Bangladesh are utilised by organised criminal gangs to smuggle counterfeit notes into India. Once smuggled, the fake money is exchanged for original notes on a roughly 2:1 ratio⁴.

24. According to the Indian authorities, proceeds of crime committed in India have been laundered in foreign jurisdictions. A number of cases of money laundering where the proceeds of crime have been transferred overseas have been observed. Based on the information of the Directorate of Enforcement (ED), the crimes being represented in this category are: drug trafficking; smuggling; false declaration of goods under export/import as part of organised crime to obtain illegally certain benefits given by the government to promote business; human trafficking; cyber fraud; identity theft and illegal control of bank accounts; counterfeiting of Indian currency and related smuggling; counterfeited credit/value cards; trafficking in wild life products; theft of objects having cultural significance and smuggling of such products to foreign countries; arms and ammunition; white collar crime; and corruption. Having regard to these modi operandi, the Prevention of Money Laundering Act (PMLA), 2002 was again amended in June 2009 to make the offence of cross border implications a scheduled offence without any monetary threshold. With this amendment to the PMLA, transnational organised crimes and money laundering should be effectively dealt with and should also facilitate greater international co-operation in tackling such transnational crimes.

25. In South Asia, human trafficking is often referred to as one of the fastest growing transnational organised crimes. Countries in South Asia, including India, serve as origin, transit and destination countries for women, children and men being trafficked⁵. The human trafficking in India is a cause of serious concern to the Government. The Government of India has adopted a multi-pronged approach to combat human trafficking and to deal with the crime of trafficking in a holistic manner. India has taken several measures for prevention and control of the crime of trafficking and to evolve an effective and comprehensive strategy encompassing rescue, relief and rehabilitation of victims besides taking deterrent action against the law violators, setting up of Anti-Trafficking *Nodal* Cell in Ministry of Home Affairs, organising training and workshops on the issue to create awareness and capacity among the law enforcement agencies. The Government has also taken special measures to prevent child trafficking. In addition, amendments are being proposed in the legal framework, namely the Immoral Traffic (Prevention) Act, 1956 to widen its scope; to focus on traffickers and make punishments more stringent for them, prevent re-victimisation of victims and to make its implementation more effective and victim-friendly. To tackle the root causes of the problem, the Government of India is also making number of socio-economic interventions to prevent circumstances and forms of exploitation of persons, especially women and children, that leads to trafficking.

⁴ B Srinivasulu, SP, Intelligence, Hyderabad: *Pak ISI Sponsored Counterfeit Currency Circulation.*

⁵ Website UNODC – South Asia: Human trafficking.

26. India has been ranked one of the five highest bribe payers among 22 countries according to Transparency International's Bribe Payers Index in 2008. India ranks 85 among 180 countries in the Corruption Perceptions Index in 2008 with a mean score of 3.4.

27. Money laundering methods are diverse. In case of domestic crimes, the most common money laundering methods are opening multiple bank accounts, intermingling criminal proceeds with assets of a legal origin, purchasing bank cheques against cash, and routing through complex legal structures. In the case of transnational organised crimes, the use of offshore corporations and trade based money laundering are some of the methods used to disguise the criminal origin of the funds.

28. Various inter-ministerial committees are in place to review the threats. The amendments to the PMLA in 2009 essentially flow from such reviews, and most of the offences mentioned in the table above are now included as predicate offences under Part A and/or C of the Schedule to the PMLA without any threshold (see Section 2.1 for more details). Moreover, the assessment of vulnerabilities in the financial sectors resulted in the inclusion of Full Fledged Money Changers (FFMCs), Money Transfer Service Providers (MTSP), such as Western Union, and International Payment Gateways (IPG), such as Visa and Master Card, under the PMLA and this most recent amendment to the PMLA came into effect on 1 June 2009.

Terrorist Financing

29. India continues to be a significant target for terrorist groups and has been the focus of numerous attacks. The bulk of terrorist activities have been orchestrated by groups and entities linked to the global Jihad with the support of external organisations including State and non-State actors. In addition, several domestic groups involved in separatism and terrorism are also active. There are no published figures of terrorist cells operating in the country.

30. *Domestic terrorist organisations:* The Indian authorities report that the principal terrorist threat emanates from the activities of groups espousing the Maoist ideology, such as Communist Party of India (Maoist) and separatist groups in some of the North Eastern States. Special structures and mechanisms (including for conflict resolution) have been established by the Government to combat these activities with considerable success.

31. *Externally based terrorist organisations:* On the other hand, external terrorist organisations operate from bases in neighbouring countries beyond the jurisdiction of the Indian legal apparatus. These include Pakistan based terrorist outfits, such as the Lashkar-e-Tayyeba, Jaish-e-Mohammed, Harkat-ul Ansar/Harkat-ul-Jihad-e-Islami. Other groups, such as the Hizbul Mujahideen, etc. are essentially Kashmir centric though their leadership is based in neighbouring countries. The Indian authorities also report that the influence and spread of the activities of the latter groups have declined substantially over the past few years.

32. In its attempt to counter terrorist financing and money laundering, the Government is particularly concerned about the 4 100 km porous India/Bangladesh border. Out of the sanctioned length of 3 436 km, 2 709 km has been fenced. India's inability to protect its porous maritime borders came to light since the perpetrators of the 26 November 2008 Mumbai attacks arrived by sea from Pakistan, with the backing of state and non state actors of Pakistan. According to the Indian authorities, the Government has taken a number of measures to strengthen its Coastal/Maritime security.

33. Correspondingly, the pattern of terrorist financing in India covers a wide spectrum. The highest threat emanates from FT issues relating to the external terrorist groups affiliated with the global Jihad. The threat is particularly high since the groups are based outside the country and operate through multiple

nodes across the world. The Indian authorities report that issues relating to domestic terrorist groups are fully monitored and the level of threat is considerably lower.

34. A threat assessment regarding terrorism and its financing is undertaken by the Ministry of Home Affairs (MHA) on a regular basis with other relevant agencies. India itself has identified the following threats as the major sources for terrorist financing:

- a. funds/resources from organisations outside India including foreign NPOs;
- b. counterfeiting of currency;
- c. criminal activities including drug trafficking and extortion;
- d. use of formal channels and new payment methods.

Based on the results of the threat assessment, it can be stated that while the threat is high from the criminal activities listed under (a) and (b), which according to the Indian authorities relate essentially to external terrorist organisations; the threat emanating from (c) and (d) is perceived by the Indian authorities to be low.

35. The Unlawful Activities (Prevention) Amendment Act, 2008 and the establishment of the National Investigation Agency (NIA) have, among other actions, further strengthened the fight against terrorism and its financing.

1.3 Overview of the Financial Sector and DNFBP

36. The Indian financial market mainly comprises three sectors *i.e.*, a) the Banking and allied financial services, (b) the Securities sector (the capital market) and (c) the Insurance sector. However, the Indian financial sector is still dominated by bank intermediation. Though the size of the capital market has significantly expanded since the beginning of financial liberalisation in the early 1990s, bank intermediation remains the dominant feature of the Indian financial system.

a. Overview of India's Financial Sector

Table: Financial activity performed by the different types of financial institutions

| FINANCIAL ACTIVITY PERFORMED BY THE FINANCIAL INSTITUTION (SEE FATF DEFINITION OF "FINANCIAL INSTITUTION") | Banks (2 288) ⁶ | Non-bank deposit takers (321) | Non-bank non-deposit taking lenders (12399) ⁷ | Money changers & MVT services (1 080) ⁸ | Securities market brokers (9 622) | Merchant Bankers (137), Registrars (71), Debenture Trustees (30), Bankers to an issue (51), Underwriters (17), Depositories (2) and Depository Participants (718) (= 1 026) | Custodians (16) | Asset Management Companies (45) and Portfolio Managers (232) (= 277) | Life Insurance Companies (22) | Non-life Insurance Companies (21) | Insurance Agents (2 939 917) | India Post Office |
|--|----------------------------|-------------------------------|--|--|-----------------------------------|---|-----------------|--|-------------------------------|-----------------------------------|------------------------------|-------------------|
| Acceptance of deposits and other funds from the public | √ | √ | | | | | | | | | | √ |
| Lending | √ | √ | √ | | | | | √ | √ | | | |
| Financial leasing | √ | √ | √ | | | | | | | | | |
| Transfer of money or value | √ | | | | | | | | | | | √ |
| Issuing and managing means of payment | √ | | | | | | | | | | | |
| Financial guarantees and commitments | √ | √ | √ | | | | | | √ | | | |
| Trading in financial instruments | √ | √ | √ | | | | | | | | | |
| Participation in securities issues and related financial services | √ | √ | √ | | | √ | | | | | | |
| Individual and collective portfolio management. | | √ | √ | | | | | √ | | | | |
| Safekeeping and administration of cash or liquid securities. | √ | | | | | | | | | | | |

⁶ The total number of 2 288 banks comprises a) Scheduled Commercial Banks = 81; b) Urban Co-operative Banks = 1 721; c) Regional Rural Banks = 84; d) State Co-operative Banks = 31; and e) Central Co-operative Banks at District level= 371.

⁷ This number does not include 44 Housing Finance Companies, which have been exempted from the regulatory purview of the RBI (provisions of Chapter IIIB of the RBI Act, 1934 as applicable to NBFCs) through RBI Notification dated 18 June 1997.

⁸ The total number of 1 080 Money changers & Money Value Transfer Services (MVTs) comprises a) Indian agents (MVT services) = 26; b) Fully Fledged Money Changers = 933; c) Authorised Dealers-Cat-II = 35 and Authorised Dealers-Cat-I = 86.

| FINANCIAL ACTIVITY PERFORMED BY THE FINANCIAL INSTITUTION (SEE FATF DEFINITION OF "FINANCIAL INSTITUTION") | Banks (2 288) ⁶ | Non-bank deposit takers (321) | Non-bank non-deposit taking lenders (12399) ⁷ | Money changers & MVT services (1 080) ⁸ | Securities market brokers (9 622) | Merchant Bankers (137), Registrars (71), Debenture Trustees (30), Bankers to an issue (51), Underwriters (17), Depositories (2) and Depository Participants (718) (= 1 026) | Custodians (16) | Asset Management Companies (45) and Portfolio Managers (232) (= 277) | Life Insurance Companies (22) | Non-life Insurance Companies (21) | Insurance Agents (2 939 917) | India Post Office |
|--|----------------------------|-------------------------------|--|--|-----------------------------------|---|-----------------|--|-------------------------------|-----------------------------------|------------------------------|--------------------|
| Other investing, administering or managing funds. | | √ | √ | | | | | √ | √ | | | |
| Underwriting and placement of life and investment-related insurance. | | | | | | | | | | | √ | √ |
| Money and currency changing. | √ | | | | | | | | | | | √ |
| Is the financial institution subject to AML/CFT requirements (Y/N)? | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Designated regulator/supervisor | RBI | RBI | RBI | RBI | SEBI | SEBI | SEBI | SEBI | IRDA | IRDA | IRDA | DEA, MOF/ RBI/IRDA |

Banking sector

37. Financial institutions are divided into various sections covering scheduled commercial banks, regional rural banks (RRBs), urban and rural co-operative banks (UCBs), non-banking financial companies (NBFCs), housing finance companies (HFCs), and development financial institutions (DFIs). These businesses are being licensed, supervised and regulated by the Reserve Bank of India (RBI).

Table: Overview of India's Banking Sector:

| Type of institution | Numbers of financial institutions as of 31 March 2009 |
|---|---|
| Public Sector Banks | 27 |
| Private Sector Banks | 22 |
| Foreign Banks | 31 |
| Regional Rural Banks | 86 |
| Local Area Banks | 4 |
| Urban Co-operative Banks | 1 721 |
| Non Banking Finance Companies (other than deposit taking) | 12 403 |
| Deposit-taking NBFCs | 336 |
| Primary Dealers | 19 |

38. **Scheduled Commercial Banks:** Commercial banks are profit-oriented institutions mainly dealing with deposit taking, lending and other fee-based businesses, pursuant to the provisions of the Banking Regulation Act, 1949. Apart from the Banking Regulation Act, which governs all the scheduled commercial banks, there are other laws governing different groups of banks. The nationalised banks are governed by two Acts: the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 and the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980. The State Bank of India and the subsidiaries of the State Bank of India are governed by two other laws: the State Bank of India Act, 1955 and the State Bank of India (Subsidiary Banks) Act, 1959. The Industrial Development Bank of India (IDBI) is governed by the Industrial Development Bank (Transfer of Undertaking and Repeal) Act, 2003. The private sector banks come under the purview of the Companies Act, 1956. The overall regulation of the banking sector is governed by the Banking Regulation Act. There are over 82 000 branches of the commercial banks throughout India.

39. **Regional Rural Banks (RRBs):** Regional Rural Banks were established under the provisions of the Regional Rural Banks Act (RRBs Act), 1976 with an objective to ensure sufficient institutional credit for agriculture and other rural sectors. The RRBs attract financial resources from rural/semi-urban areas and grant loans and advances mostly to small and marginal farmers, agricultural labourers and rural artisans. The area of operation of RRBs is limited to the area as notified by the Government of India covering one or more districts in a State. RRBs are jointly owned by the Government of India, the concerned State Government and the sponsoring banks (26 scheduled commercial banks and one state co-operative bank). On 31 March 2009, there were 86 RRBs covering 615 districts with a network of 15 107 branches. The RRBs are also regulated by the RBI under the Banking Regulation Act, the RBI Act and the RRBs Act.

40. **Urban and Rural Co-operative Banks (UCBs and RCBs):** The co-operative banks are important parts of the Indian financial system. They play a significant role in agricultural credit in rural areas and in financing the credit needs of small borrowers in urban areas. Rural co-operative banks comprise State Co-operative Banks (StCBs) and Central Co-operative Banks at District level (DCCBs). These banks are governed by the Banking Regulation Act and the Banking Laws (Co-operative Societies) Act, 1965 and are registered under the Co-operative Societies Act of the concerned State. Supervisory functions (including statutory inspection) in respect of rural co-operative banks are vested with the National Bank for Agriculture and Rural Development (NABARD), while regulatory functions are with the RBI under the Banking Regulation Act. The business of co-operative banks in the urban areas has increased phenomenally in recent years. The Urban Co-operative Banks are registered under the Co-operative Societies Act of the State concerned or the Multi-State Co-operative Societies Act, 2002 and are governed by the Banking Regulation Act and the Banking Laws (Co-operative Societies) Act, 1965. The Reserve Bank of India regulates and supervises (including statutory inspection) the UCBs under the powers vested in it by the Banking Regulation Act.

41. **Non-Banking Financial Companies (NBFCs):** A Non-Banking Financial Company is a company registered under the Companies Act and is engaged in the business of loans and advances, acquisition of shares/stocks/bonds/debentures/securities issued by the Government or a local authority or other securities, leasing, hire-purchase, and chit business⁹. NBFCs do not include any institution whose principal business is that of agricultural activity, industrial activity, purchase or sale of any goods other

⁹ "Chit" means a transaction whether called chit, chit fund, chitty, kuri or by any other name or under which a person enters into an agreement with a specified number of persons that every one of them shall subscribe a certain sum of money (or a certain quantity of grain instead) by way of periodical instalments over a definite period and that each such subscriber shall, in his turn, as determined by lot or by auction or by tender or in such other manner as may be specified in the chit agreement, be entitled to the prize amount (section 2(b) of the Chit Funds Act, 1982).

than securities or providing of any service, sale/purchase/construction of immoveable property. A non-banking institution which is a company and whose principal business is receiving deposits under any scheme or arrangement or in any other manner, or lending in any manner is also a non-banking financial company (a residuary non-banking company). Under the Reserve Bank of India Act, 1934 (RBI Act), it is mandatory that every NBFC be registered with the RBI before it can commence or carry on any business of an NBFC. However, the RBI has exempted certain categories of NBFCs such as Insurance companies, chits¹⁰, etc. from registration. The NBFCs may further be classified into two types: those accepting deposits and those not accepting deposits.

42. **Housing Finance Companies (HFCs):** A Housing Finance Company includes every institution, whether incorporated or not, which primarily transacts or has as one of its principal objects, the transacting of the business of providing finance for housing, whether directly or indirectly.

43. **Developmental Financial Institutions (DFIs):** Developmental Financial Institutions have been established and capitalised by the Central Government. These DFIs participate in the financing and credit businesses related to the Government's economic policies. DFIs are non-commercial financial institutions. The DFIs are the National Bank for Agriculture and Rural Development (NABARD), the National Housing Bank (NHB), the Export Import Bank of India (EIBI) and the Small Industries Development Bank of India (SIDBI):

- a. **The National Bank for Agriculture and Rural Development (NABARD):** The NABARD is set up as a development bank with a mandate for facilitating credit flow for promotion and development of agriculture, small-scale industries, cottage and village industries, handicrafts and other rural crafts. It is also mandated to support all other allied economic activities in rural areas, promote integrated and sustainable rural development and secure prosperity of rural masses. As an apex bank, it is also involved in refinancing credit needs of major financial institutions in the country engaged in offering financial assistance to agriculture and rural development operations and programmes.
- b. **The National Housing Bank (NHB):** The NHB was established under the National Housing Bank Act, 1987 (NHB Act) as a wholly owned subsidiary of the RBI to function as a principal agency to promote housing finance institutions and to provide financial and other support to such institutions. The NHB provides loans and advances and other forms of financial assistance to scheduled commercial banks, housing finance institutions or other specified authorities for the purpose of mobilisation of resources and extension of credit to housing.
- c. **The Export Import Bank of India (Exim Bank):** The major objective of the Exim Bank is to provide economic assistance to importers and exporters and to function as a top financial institution in financing of exports and imports. Some of the important services of the Bank include export credit, overseas investment financing Small and Medium Enterprises (SMEs) finance, film finance, and financing of export-oriented units and providing lines of credit to foreign countries and overseas entities to promote domestic exports.
- d. **The Small Industries Development Bank of India (SIDBI):** The SIDBI was set up in order to be the principal financial institution for the promotion, financing and development of small scale industries and to co-ordinate the functions of the institutions engaged in the promotion, financing and development of small scale industries.

¹⁰

Chit companies doing the business of chits as defined in clause (b) of section 2 of the Chit Funds Act, 1982, are exempted from the provisions of section 45-IA (requirement of registration), section 45-IB (maintenance of liquid assets), and section 45-IC (creation of reserve fund) of the RBI Act, 1934. Chit companies are registered and regulated by the respective State Governments (Registrar of Chits).

Foreign Exchange Market

44. Although the foreign exchange markets have been liberalised in recent years, foreign currency transactions may only be undertaken through banks, and money changers so authorised by the RBI under the Foreign Exchange Management Act, 1999 (FEMA). This Act partly liberalised the control on foreign exchange in 1999, and replaced the criminal framework for breaches of the controls (contained in the previous Foreign Exchange Regulation Act, 1973 – FERA) with provisions for administrative and civil sanctions.

Securities sector

45. The Indian financial markets can be broadly categorised into the money market, the foreign exchange market, the government securities market, the equity market, the corporate bond market and the credit market. While foreign exchange, government securities, equity and money markets along with their corresponding derivatives segments have developed into reasonably deep and liquid markets, credit derivatives markets are yet to take off in any significant manner.

46. The securities sector in India comprises various Intermediaries as registered under section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act). The following table sets out an overview of the different types of intermediaries that constitute the securities sector:

| Regulated entities | Number as on 31 March | | |
|--|-----------------------|--------|--------|
| | 2007 | 2008 | 2009 |
| Registrar to an Issue and Share Transfer Agent | 82 | 76 | 71 |
| Banker to an Issue | 47 | 50 | 51 |
| Debenture Trustee | 30 | 28 | 30 |
| Merchant Banker | 152 | 155 | 137 |
| Portfolio Manager | 158 | 205 | 232 |
| Underwriter | 45 | 35 | 17 |
| Depositories | 2 | 2 | 2 |
| Depositories Participants | 593 | 654 | 718 |
| Credit Rating Agency | 4 | 5 | 5 |
| Registered Stock Brokers | 9 443 | 9 487 | 9 622 |
| Registered Sub-brokers | 27 541 | 44 074 | 62 761 |
| Stock Exchange | 21 | 19 | 19 |
| Foreign Institutional Investors | 996 | 1319 | 1635 |
| Custodians | 15 | 15 | 16 |
| Collective investment schemes including mutual funds | 40 | 40 | 45 |
| Venture Capital Funds | 90 | 106 | 133 |
| Foreign Venture Capital Investors | 78 | 97 | 129 |

47. In India “Securities” include shares, stocks, debentures, bonds, Pass-Through Certificates (PTCs), and government securities and mutual fund units. India has adopted the “depository system”, in which depositories function as the central accounting and record-keeping office in respect of the securities admitted by issuer companies. Companies which issue any kind of securities are known as 'Issuer' in the depository system. Both listed and unlisted securities can be admitted into the depository system. Only

these securities admitted into the depository system are available for dematerialisation to the holders of such securities or can be allotted in electronic record form by the issuers. A depository is thus a "service centre" for the investor and the depositories system is based on centralised database architecture with on-line connectivity for depository participants.

Secondary Market

48. Although there are 19 exchanges across the country, only two of these have any significant volume of activity. There are two stock exchanges that account for nearly all the transactions in the equity and derivative segments, the Bombay Stock Exchange (BSE) and the National Stock Exchange (NSE). Both exchanges are using computer based anonymous trading platforms for over a decade. The stock exchanges have powers to ensure that their members adhere to prescribed regulations and instructions. The use of cash for payments has been removed and all payments now take place either through cheques or through electronic payments. Apart from investments by natural and legal persons based in the country, money from abroad enters the capital markets through the vehicle of Foreign Institutional Investors (FII) that are registered by SEBI prior to their entry.

Insurance Sector

49. The insurance sector was opened for private participation with the enactment of the Insurance Regulatory and Development Authority Act, 1999 (IRDA Act) and the establishment of a separate regulator for the insurance sector, the Insurance Regulatory and Development Authority (IRDA). The legislative framework for this sector is contained in the Insurance Act, 1938 and the IRDA Act. Since the opening up, the number of participants in the industry has increased from six wholly public owned insurers (comprising the Life Insurance Corporation of India (LIC); the four general insurance companies; the national reinsurer; and the General Insurance Corporation) in 2000 to 44 insurers/reinsurer operating in the life, general and re-insurance segments on 31 March 2009 (including the public sector insurers).

Table: Break-down of public and private sector companies in the insurance sector

| Type of business | Public Sector | Private Sector | Total |
|-------------------|---------------|----------------|-----------|
| Life Insurance | 1 | 22 | 23 |
| General Insurance | 6 | 16 | 22 |
| Re-insurance | 1 | -0 | 1 |
| Total | 8 | 38 | 46 |

Department of Posts

50. The Department of Posts is a government department under the Ministry of Communications and Information Technology which is mandated to manage the postal operations of India, the postal retail network, and small savings deposit activity under various Acts, ranging from the Post Office Act, 1898 to the Government Savings Act, 1873. Post offices are located in both rural and urban areas.

51. The Department of Posts operates under the informal brand name "India Post" and provides a range of financial services, including savings and deposit accounts, life insurance, mutual funds and money remittance within India (through the issuance of money orders). The India Post website states that it is the largest retail bank in the country operating 220 million savings accounts from 150 000 branches. These deposit-taking activities are not covered by the primary banking or financial services laws, but are, as indicated above, governed by the Government Savings Bank Act. However, since India Post is a "financial institution" for the purposes of the PMLA (by reason of being an Authorised Person with respect to its foreign exchange operations), all its financial services activities are subject to the provisions of the PMLA.

Despite this, India Post is not supervised by the mainstream financial services regulators (except for its foreign exchange business), and, this role falls, instead, to the Ministry of Finance audit department.

Offshore Financial Services

52. Although India does not play host to offshore financial services in the traditional sense, it has made provision for Offshore Banking Units (OBUs) to operate in the Special Economic Zones (SEZs) that are being established to promote export-oriented commercial businesses under the Special Economic Zones Act, 2005. At the time of the on-site visit, 346 SEZs had been nominated throughout India, providing both multi-sector and specialist access. The scope of activities includes manufacturing, trading and services (mostly information technology). The SEZs have defined physical boundaries, to which access is controlled by Customs officers. Seven OBUs have been set up in specific zones, although they can provide services across the entire network. Of the seven, as at the time of the on-site visit, six OBUs exist. These units are prohibited from engaging in cash transactions and are restricted to lending to the units located in the SEZs. They virtually function as foreign branches of Indian banks, but are located in India. OBUs are licensed and regulated prudentially by the RBI on the same lines as the domestic commercial banks, and are subject to the same AML/CFT provisions as the domestic sector.

b. Overview of designated non-financial businesses and professions (DNFBP)

Table: Types and numbers of designated non-financial businesses and professions (DNFBP)

| Type of institution | Number present in India | Are these DNFBP subject to AML/CFT requirements (Yes/No)? | Supervisor/Regulator |
|---------------------------------------|--|---|---|
| Casinos | 20 | Yes | State Home Department of the Goa Government |
| Real estate agents | No official estimates are available. | No | None |
| Dealers in precious metals and stones | No official estimates are available* | No | None |
| Lawyers | +/- 1 050 000 Advocates | No | The Bar Council of India |
| Accountants | - +/- 145 000 Chartered Accountants - +/- 40 000 Cost Accountants | No | <ul style="list-style-type: none"> • The Institute of Chartered Accountants of India (ICAI) for Chartered Accountants • The Institute of Cost and Works Accountants of India (ICWAI) for Cost Accountants |

* As per Report on Gems and Jewellery (May 2004) by the India Brand Equity Foundation which is a public - private partnership between the Ministry of Commerce, Government of India, and the Confederation of Indian Industry, jewellery is sold across 300 000 outlets.

** Lawyers in India are prohibited from facilitating any financial transactions for their clients.

*** Number of practising lawyers/accountants is lower.

Casinos

53. Casinos are not legal in India except in the State of Goa where the Goa Public Gambling Act, 1976 has been amended to permit the operation, in a restricted manner, of land-based and offshore casinos.

54. The Home Department of the Government of Goa issues licences to casinos and, at the time of the on-site visit, it had issued licences for 14 land-based casinos (located in five-star hotels) and 6 offshore (ship-based) casinos, although only eleven onshore and three offshore operators had started business. Offshore casinos must also be licensed by the Director General of Shipping at the Ministry of Surface Transport, and must also possess a certificate of non-objection from the Captain of Ports. Onshore casinos are prohibited from providing live tables, and are restricted to offering slot machines and electronic games. Offshore casinos are able to provide live tables, but the gambling activities are primarily incidental to the dining and entertainment facilities on the ships. The casinos were brought within the PMLA framework via the amendments to the PMLA, which came into force on 1 June 2009.

Real estate agents

55. The Indian authorities describe the real estate agents as an “un-organised sector”, in that there is no universal requirement to be registered or licensed, and the role of the agent is ill-defined. Regulation of land/real estate development is within the States’ powers. Real estate deals are negotiated directly between the sellers and buyers, but may be facilitated by brokers, who act as self-appointed intermediaries between the parties and help them to complete the deal. The agent has no contractual relationship with either party, and may be paid by either the buyer or the seller, or by both. Real estate agents operate mostly on an individual basis and real estate companies are rather exceptional. All real estate transactions are registered under the departments of the State Government in whose jurisdiction the transactions fall.

Dealers in precious metals and precious stones

56. Gold dealers are subject to an import regime, and must be registered entities (nominating agencies) with the RBI to transact payments for gold purchases. Retailers must go through a ‘nominating agency’, whose licensees are publicly listed. There exist about 20 nominating entities with associated accounts, through which gold can be purchased. These ‘nominating agencies’ are government or trading monopolies, and are either associated banks or agencies. Trading monopolies must set up a Limited Liability Company (LLC) with an established bank account in order to deliver gold to a purchaser on request. Banks and Agencies must keep on hand a list of approved gold exporters from whom to purchase.

57. The RBI oversees the gem and jewellery sector from the standpoint of the export/bank finance side, and therefore must conduct KYC on wholesale account holders. All transactions are financed through banking channels, and gem and jewellery exporters are not permitted to accept cash pursuant to the FEMA provisions. All dealers in precious metals and stones are required to register themselves with the respective State Government’s Commercial Taxes Departments.

Lawyers

58. Lawyers are a uniquely governed profession in India. The Bar Council of India – separated into State level offices – oversees the enrolment of lawyers, looks after their interests, and carries out disciplinary actions. There are no mandatory continuing education obligations for renewal of licenses. Lawyers do not handle business outside the legal obligations to their client, and therefore do not engage in financial transactions on behalf of their clients. The assessment team was told that lawyers were prohibited from facilitating any financial transactions for their clients (although the basis for this prohibition is unclear), but they do routinely hold funds on deposit and in escrow for their clients. There exists a separate role for solicitation, and fees are not allowed to be paid on a contingency basis.

59. The legal profession is governed by the Advocates Act, 1961. Two or more advocates may constitute a partnership firm, whose membership cannot exceed twenty. Except in some metropolitan cities, partnership firms among lawyers are not very common and the profession consists of mostly individual practices. A person can practice as an advocate (lawyer) only if he is registered with the Bar Council of India (BCI). The BCI, constituted under the Advocates Act, is a self-regulatory organisation for

lawyers. Among other things, it has laid down standards of professional conduct and etiquette and standards of legal education. The BCI does registration of advocates; and enforcement of discipline among the lawyers. It also exercises appellate jurisdiction and constitutes the Disciplinary Committees.

60. The advocates are authorised to appear in all courts, tribunals and other authorities unless specifically prohibited. Solicitors and attorneys function as independent legal professionals in some of the High Courts of the country and, if they are advocates, they are regulated by the Advocates Act.

Notaries

61. Notaries in India are also lawyers, but are regulated under the Notaries Act, 1955 and are appointed by either the Central Government or one of the State Governments. Their role is limited to attesting documents and affidavits, verifying the legality, objectivity and authenticity of documents and transactions, and endorsing, noting and protesting in respect of bills of exchange. These activities are exercised in addition to their usual activity as lawyers.

Chartered Accountants

62. The chartered accountants are regulated by the Institute of Chartered Accounts of India (ICAI), which is the statutory body established under the Chartered Accountants Act, 1949. Apart from auditing or verification of financial transactions, books, accounts or records, or the preparation, verification or certification of financial accounting and related statements, chartered accountants are legally permitted to render "Management Consultancy and other Service". This activity encompasses (but is not limited to) the following services: (a) financial management planning and financial policy determination; (b) capital structure planning and advice regarding raising finance; (c) preparing project reports and feasibility studies; (d) investment counselling in respect of securities as defined in the Securities Contracts (Regulation) Act, 1956 and other financial instruments; and (e) acting as registrar to an issue and for transfer of shares/other securities. Practicing without being a member of the ICAI is a criminal offence. On 31 March 2009, there were 145 481 chartered accountants in India, out of which 77 814 were in practice. There are a total of 34 706 firms of chartered accountants.

Cost and Works Accountants (CWAs)

63. A Cost and Works Accountant is a person who offers to perform or performs services involving the costing or pricing of goods and services or the preparation, verification or certification of cost accounting and related statements. The Institute of Cost and Works Accountants of India (ICWAI) is the only recognised statutory professional organisation and licensing body in India specialising exclusively in cost and management accountancy. The profession was established by the Cost and Works Accountants Act, 1959.

Company service providers (CSP)/Trust service providers (TSP)

64. The company secretaries are regulated by the Institute of Company Secretaries of India (ICSI), which was set up under the Company Secretaries Act, 1980. Company secretaries are legally authorised to render the following services: (a) promotion, forming, incorporation, amalgamation, reconstruction, reorganisation or winding up of companies; (b) filing, registering, presenting, attesting or verifying any documents (including forms, applications and returns) by or on behalf of the company; (c) rendering services as may be performed by a share transfer agent, an issue house, a share and stock broker, an advisor, and an adviser to a company under relevant Acts; and (d) issuing certificates on behalf of, or for the purpose of, a company.

65. No member of the Institute is entitled to practice, whether in India or elsewhere, unless he has obtained a Certificate of Practice from the Council. However, there is no prohibition on someone holding

themselves out to be a company secretary without being a member of the ICSI. A practicing member of the ICSI is not allowed to engage in any business or occupation other than the profession of company secretary, without obtaining the prior permission of the ICSI Council.

66. Trust and Company Service Providers (TCSPs) is not a distinct business sector in India, and the activities usually associated with such a business are typically provided by accountants and company secretaries. Institutions can, however, act as debenture trustees and provide other types of fiduciary/trust services in the securities sector. These types of trust companies also act as trustees under the Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 and provide services for establishing and administering trusts. They are required to be licensed by the SEBI, are covered under the PMLA in the category of “intermediaries”, and are subject to the PMLA provisions and the SEBI circulars.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

67. The General Clauses Act, 1897 (GCA) defines ‘person’ to include any company or association or body of individuals, whether incorporated or not. There are several primary business entities in India, each governed by separate statutory regimes. The list of business entities and the governing statutes is set out in the table below:

| Business Entities | Governing Statutes |
|-------------------------------|--|
| Company | Companies Act, 1956 |
| Limited liability partnership | Limited Liability Partnership Act, 2008 |
| Partnership Firm | Indian Partnership Act, 1932 |
| Sole proprietorship Firms | Laws Applicable to the proprietor of the firm |
| Hindu Undivided Firms | Hindu Laws |
| Co-operative Societies | Multi-State Co-operative Societies Act, 2002 and the States’ Co-operative Societies Acts |

Companies

68. Companies are created, registered and regulated under the Companies Act, 1956. Private limited companies may have two to fifty members whereas public companies must have a minimum of seven members with no limit on the maximum number. The shares of public companies may be either unlisted or listed. In the latter case they are traded on one or more of the country’s stock exchanges. All companies, whether private or public, have to provide a Memorandum of Association and Articles of Association which are filed with the Registrar of Companies in the State in which the Registered Office of the company is proposed to be situated. There were 786 774 active limited companies on 31 March 2009. These comprised 785 183 non-government companies and 1 591 government companies. Out of the 786 774 companies which are limited by shares, 82 058 companies are public limited and 704 716 are private limited companies. On 31 March 2009, there were 2 903 established places of business by foreign companies in India, as defined under section 591 of the Companies Act.

Limited Liabilities Partnership Concerns (LLPCs)

69. The concept of Limited Liabilities Partnership Concerns has recently been introduced in India by the enactment of the Limited Liabilities Partnership Act, 2008. This Act was recently enacted and is meant to facilitate the formation of LLPCs.

Partnership concerns

70. Partnership concerns are the most common form of business entities in India, particularly for small business enterprises. Partnership firms are constituted and registered under the provisions of the Partnership Act, 1932. The Act provides for registration of the firms with the Registrar of Firms appointed by the respective State Governments; however, registration of a partnership firm is optional. A minimum two persons can form a firm and the number of partners is limited to ten in the case of banking business and 20 in case of any other kind of business. Otherwise, they will be considered as an illegal association pursuant to section 11 of the Companies Act. A company can also join a partnership firm and become a partner of the firm.

Sole Proprietorship Firms

71. A person can form a sole proprietorship firm and act as proprietor of the firm. It is not a separate legal entity from the beneficial owner/proprietor of the firm and the person is doing some business under an assumed name. The proprietor is solely responsible for all acts and liabilities of the firm.

Hindu Undivided Family (HUF)

72. Hindu Personal Law recognises the institution of a HUF Business headed by the Karta/Manager of the HUF, who generally is the father or the eldest male member of the HUF. A HUF consists of father, brothers, sons, male lineal descendants, their spouses and unmarried daughters. The property of the family, which can be held in the name of any member, is supposed to be common and the members acquire right to share by birth and marriage. Being part of customary personal law, no separate document is required to be executed for its creation or continuance. However, the banks insist on disclosure of information as to membership while opening an account.

Co-operative societies

73. Any group of persons with a common economic interest or disability may constitute themselves into a co-operative society. Co-operative societies are regulated under the States' Co-operative Societies Acts. Co-operative societies having businesses in more than one State are governed by the Central Multi-State Co-operative Societies Act, 2002. Farmers, artisans, landless labourers, urban and rural workers have formed co-operative societies for collective businesses on a one member, one vote structure. The basic documents for registration of a co-operative society are the Memorandum and Articles of Association.

Non-Profit Organisation (NPO)/ Non-Government Organisations (NGO)/ Foundation

74. A NGO/NPO/foundation is a non-profit legal person that makes use of property which has been donated by natural persons, legal persons, or other organisations for the purpose of pursuing welfare undertakings. They can be registered either as an unlimited company under section 25 of the Companies Act or a society under the Societies Registration Act, 1860. Some charities function as trusts; in that case the trust deed is registered with the Registrar of Assurances. In addition, Muslim families in India can create a wakf¹¹ for religious and charitable purposes.

¹¹ A "wakf" is a charitable Islamic trust that involves "the permanent dedication by a person professing Islam of any moveable or immoveable property for any purpose recognised by the Muslim law as pious, religious or charitable".

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

75. India's anti-money laundering regime is centred on the Prevention of Money Laundering Act, 2002 (PMLA). The PMLA has been further amended by the Prevention of Money Laundering Amendment Act, 2005 and the Prevention of Money Laundering Amendment Act, 2009. The formal objective of the PMLA is to prevent money laundering and to provide for confiscation of property derived from or involved in money laundering. The Unlawful Activities (Prevention) Act, 1967 (UAPA) tackles the matters relating to terrorism and its financing. The UAPA was amended in 2004 to criminalise, inter alia, terrorist financing. The UAPA has been further amended by the Unlawful Activities (Prevention) Amendment Act, 2008 to strengthen the fight against terrorism and terrorist financing.

76. India has adopted a multi-pronged approach to respond to ML/FT risks, as identified in Section 1.2 above. India considers the key elements of its overall strategy for combating money laundering and terrorist financing to be as follows:

- a. ensuring effective supervision of financial institutions operating in India;
- b. ensuring compliance of reporting entities with the requirements of the PMLA;
- c. establishing an effective law enforcement system that is deterrent;
- d. strengthen organisational capacity of law enforcement/intelligence agencies;
- e. establishing an effective co-ordination mechanism between agencies;
- f. supporting international AML/CFT efforts and co-operation;
- g. implementing an inter-ministerial mechanism for policy co-ordination;
- h. reviewing and strengthening the legal and regulatory framework; and
- i. implementing international AML/CFT standards, particularly the FATF 40+9 Recommendations.

b. The institutional framework for combating money laundering and terrorist financing

Policy Agencies: Ministries and co-ordinating committees

77. The **Economic Intelligence Council (EIC)**: The EIC is the mechanism in place since 2003 for domestic co-operation and co-ordination. It is chaired by the Minister of Finance and further comprises the most senior functionaries of various Ministries and intelligence agencies; and the Governor of the RBI and the Chairman of the SEBI. The EIC meets at least once a year to discuss and take decisions regarding trends in economic offences, strategies on intelligence sharing, co-ordination, etc. The implementation of decisions taken by the EIC is monitored by the Working Group on Intelligence Apparatus, set up for this purpose within the EIC.

78. The **Inter-Ministerial Co-ordination Committee on Combating Financing of Terrorism and Prevention of Money Laundering (IMCC)**: The IMCC has been set up in 2002 to ensure effective co-ordination between all competent authorities and strengthening India's national capacity for implementing AML/CFT measures which meet international standards. The IMCC is chaired by the Additional Secretary of the Department of Economic Affairs within the Ministry of Finance. At present the committee consists of 14 agencies with a substantial role in AML/CFT.

79. The **Ministry of Finance (MOF)**: The MOF is the central Ministry responsible for India's fiscal policies, including revenue and tax collection, budgeting and expenditure of the Government. The MOF consists of the Department of Economic Affairs, the Department of Revenue, the Department of

Expenditure, the Department of Financial Services, and the Department of Disinvestments. The MOF is also the parent Ministry for the Directorate of Enforcement, the Central Board of Direct Taxes, the Central Board of Excise and Customs, the Central Economic Intelligence Bureau, and the Central Bureau of Narcotics. The MOF is responsible for exercising regulatory and supervisory control over the AML/CFT strategies. The following agencies are relevant in India's AML/CFT framework:

- a. The ***Department of Economic Affairs (DEA)***: The DEA is the principal agency of the Union Government to formulate and monitor the country's economic policies and programmes having an impact on domestic and international aspects of economic management. The principal responsibility of this Department is the preparation of the Union Budget annually (excluding the Railway Budget). The DEA has a co-ordinating role within the Government of India regarding the Financial Action Task Force (FATF).
- b. The ***Department of Revenue (DOR)***: The DOR functions under the overall direction and control of the Secretary of Revenue and exercises control over the matters related to all the direct and indirect Union taxes through two statutory Bodies namely, the Central Board of Direct Taxes (CBDT) and the Central Board of Excise and Customs (CBEC). One of the main regulatory statutes under the DOR is the PMLA and the DOR is in charge of ensuring the implementation of AML measures.
- c. The ***Department of Financial Services (DFS)***: The DFS is the policy making body for the banking, insurance and pension sectors. Its Banking Division administers policies related to the banks and the lending financial institutions. The Insurance Division has close ties with the Insurance Regulatory and Development Authority (IRDA), the AML/CFT supervisor for the insurance industry.

80. The ***Ministry of Home Affairs (MHA)***: The MHA is the *nodal* Ministry for combating terrorism in all its manifestations and is also responsible for the general maintenance of Internal Security in the Country. The MHA also administers various security, investigative and law enforcement agencies such as the National Investigation Agency, the Narcotics Control Bureau, and the Intelligence Bureau. Moreover, India's CFT legislation (UAPA) and the National Investigation Agency Act, 2008 (NIA Act), constituting the National Investigation Agency (NIA - see below) are administered by the MHA.

81. The ***Ministry of External Affairs (MEA)***: The Ministry of External Affairs is responsible for all aspects of relations with other countries. The major area of work of the MEA is as follows:

- a. external affairs, relations with foreign states and commonwealth countries;
- b. all matters related to foreign diplomatic and consular officers, U.N. offices and its specialised agencies in India, passports and visas;
- c. extradition of criminals and accused persons from India to foreign and commonwealth countries and vice versa; the general administration of the Extradition Act, 1962; and extra-territoriality;
- d. repatriation of the foreign and commonwealth States' nationals from India and deportation and repatriation of Indian nationals from foreign and commonwealth countries to India;
- e. political treaties, agreements and conventions with foreign and commonwealth countries and foreign jurisdictions;
- f. all consular functions;
- g. ceremonial matters relating to foreign and commonwealth visitors and diplomatic and consular representatives; and

- h. U.N. specialised agencies and other international organisations, including India's NCB Interpol office; and conferences.

82. The **Ministry of Law and Justice (MLJ)**: The MLJ gives advice to Ministries on legal matters, including interpretation of the Constitution and the laws. It also provides legal advice to government departments and law enforcement agencies on the interpretation of AML/CFT laws and issues; legal policies on civil and criminal justice; and alternative dispute resolution. The MLJ is also responsible for advising the Government on all domestic law/legal matters. In addition, the MLJ does conveyance and engagement of counsels to appear on behalf of the Union of India in the High Courts and Subordinate Courts where the Union of India is a party. The Attorney General of India, the Solicitor General of India, and other Central Government law officers are appointed by the MLJ. The MLJ also regulates the legal profession, including the Advocates Act and persons entitled to practice before High Courts in India; it administers the Notaries Act and provides legal aid to the poor. The Legal and Treaties Division, Ministry of External Affairs, advises the Government of India on all international legal matters.

83. The **Ministry of Corporate Affairs (MCA)**: The MCA is primarily concerned with the administration of the Companies Act; other allied Acts and rules and regulations framed there-under mainly for regulating the functions of the corporate sector in India. The Ministry is also responsible for administering the Partnership Act; the Societies Registration Act; Limited Liability Partnership Act, 2008 and the Competition Act, 2002. The MCA exercises supervision over three professional bodies, namely, the ICAI, the ICSI and ICWAI, which are constituted under three separate Acts (see above).

Criminal Justice and Operational Agencies

84. The **Directorate of Enforcement (ED)**: The ED is the government agency which was established in 1956 and has currently been entrusted with the investigation and prosecution of money laundering offences and attachment/confiscation of the proceeds of crime under the PMLA. The officers of the ED undertake multifaceted functions of collection, collation and development of intelligence, investigation into suspected cases of money laundering, attachment/confiscation of the assets acquired from the commission of scheduled offences, and the criminal prosecution of the offenders in the court of law. The ED also enforces the provisions of the FEMA, aimed at promoting the development and maintenance of India's foreign exchange market, and providing, inter alia, for action against persons/entities involved in international *Hawala* transactions (cases of financial transactions through alternate remittance systems between parties in India and those in other countries).

85. The ED has a pan-Indian character with 21 field offices spread over various States and Regions in India. There is a separate legal wing headed by a Prosecutor, with two deputy legal advisers and 10 assistant legal advisers who render legal advice to the officers of the ED. Additionally, the ED relies on the services/expertise of eminent legal experts and Public Prosecutors for general advice and guidance as well as regarding the presentation of the ED's cases in various courts and legal fora.

86. The **Financial Intelligence Unit-India (FIU-IND)**: The FIU-IND was set up by the Government of India through its Office Memorandum of 18 November 2004 and became operational in March 2006. The FIU-IND has been designated as the central national agency for receiving, processing, analysing and disseminating information relating to suspect financial transactions as well as large cash transactions. In addition, the FIU-IND is responsible for co-ordinating and strengthening efforts of national and international intelligence, investigating and enforcement agencies in pursuing the global efforts against money laundering, terrorist financing and other related crimes.

87. The **Central Economic Intelligence Bureau (CEIB)**: The CEIB provides a link between the EIC and the operations of enforcement agencies. It was set up as a result of the recommendations of the Group of Ministers for co-ordinating and strengthening the intelligence gathering activities and enforcement

action by various agencies concerned with investigation into economic offences and enforcement of economic laws. Under the CEIB, 18 Regional Economic Intelligence Councils (REICs) have been set up across the country for further co-ordinating the work among various enforcement and investigating agencies dealing with economic offences. The Revenue Secretary, who is the Chairman of the Working Group on Intelligence Apparatus (see above), periodically reviews the functioning and effectiveness of the co-ordination between the CEIB, the ED and the FIU-IND and other agencies.

88. The **National Investigation Agency (NIA)**: Under the National Investigation Agency Act (NIA Act), the Central Government has set up a federal, specialised and dedicated investigating agency, the NIA, to investigate and prosecute scheduled offences, in particular the offences under the UAPA, including FT offences. The NIA has concurrent jurisdiction with the individual States, and this empowers the Central Government to probe terror attacks in any part of the country. Officers of the NIA have all powers, privileges and liabilities which police officers have in connection with investigation of any offence. The NIA Act empowers the Central Government to *suo motu* assign a case to the NIA and at the time of the on-site visit; three cases were assigned to the NIA for investigation. The NIA Act also provides for setting up of Special Courts, and trials to be held on a day-to-day basis.

89. The **Central Bureau of Investigation (CBI)**: The CBI plays an important role in international co-operation, in particular mutual legal assistance and extradition matters. The Ministry of Home Affairs is the central authority for Mutual Legal Assistance in criminal matters and the Ministry of External Affairs is the *nodal* agency for extradition matters. The CBI derives its jurisdiction and powers from the Delhi Special Police Establishment Act, 1946 (DSPEA). The main divisions of CBI are the:

- a. anti-corruption division;
- b. economic offences division;
- c. special crimes division;
- d. directorate of prosecution;
- e. administration division;
- f. policy and co-ordination division;
- g. central forensic science laboratory.

90. The CBI is the premier investigating agency of the country and the organisation has evolved from an anti-corruption agency to a multi-disciplinary central law enforcement agency with legal mandate to investigate and prosecute offences anywhere in India. The CBI is also responsible for enforcing the Prevention of Corruption Act, 1988 in relation to corruption and corrupt practices by officials of the Central Government and the Central Government undertakings/bodies/organisations.

91. The **Narcotics Control Bureau (NCB)**: The NCB is an apex co-ordinating agency. The broad legislative policy is contained in the three Central Acts: the Drugs and Cosmetics Act, 1940; the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act); and the Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, 1988. The NCB operates under the administrative control of the MHA. The NCB is also responsible for investigation of cases under the NDPS Act and filing of complaints in court. It has preventive and enforcement functions, and can undertake action for tracing and freezing of illegally acquired property pursuant to the provisions of Chapter VA of the NDPS Act.

92. The **Central Bureau of Narcotics (CBN)**: The CBN supervises the licit cultivation of opium poppy in India, issues licences for manufacture of synthetic narcotics drugs and export authorisations/imports certificates for export/import of licit narcotics drugs and psychotropic substances. It monitors India's implementation of the United Nations Drug Control Conventions. Moreover, it interacts

with the International Narcotics Control Board (INCB) in Vienna and the competent authorities of other countries to verify the genuineness of a transaction prior to authorising the shipments.

93. The **Bureau of Immigration (BOI)**: There are 78 Immigration Check Posts (ICPs) in the country out of which 26 are airport ICPs, 20 are seaport ICPs and 32 are land ICPs. Out of these 78 ICPs, 12 are controlled by the BOI, while the remaining 66 ICPs are managed by the State Governments as agencies of the Government of India. Immigration checks are conducted at the ICPs for all passengers, Indians and foreigners, both at the time of arrival and departure. All passengers coming to India or departing from India are also required to complete D- (Disembarkation) and E- (Embarkation) Cards on arrival and departure respectively.

94. The **Serious Frauds Investigation Office (SFIO)**: The SFIO has been set up by the Government of India in the MCA to investigate corporate frauds of serious and complex nature. So far, the SFIO has conducted investigations in 49 cases.

95. The **Central Board of Direct Taxes (CBDT)**: The CBDT is a statutory authority functioning under the Central Board of Revenue Act, 1963. The Board comprises of a Chairman and six members. The Board is assisted by a secretariat in the discharge of its functions. The Board administers all matters relating to direct taxes through the Income Tax Department (ITD). The ITD has a dedicated investigation wing with offices all over the country. Moreover, the ITD also has a dedicated wing to deal with tax matters of NPOs, which includes, inter alia, the work of registering and granting exemptions to NPOs/Charities from income tax (see also Section 5 of this report).

96. The **Central Board of Excise and Customs (CBEC)**: The CBEC is a statutory authority functioning under the Central Board of Revenue Act. The CBEC is a part of the DOR and deals with the tasks of formulation of policy concerning levy and collection of customs and Central excise duties and service tax. It is also in charge of the prevention of smuggling and is responsible for the administration of the declaration system and the enforcement of laws regarding the physical cross-border transportation of currency or bearer negotiable instruments (BNI).

- a. The **Directorate of Revenue intelligence (DRI)**: The DRI functions under the CBEC and is in its present form a lean organisation charged essentially with the collection of intelligence, analysis, collation, interpretation and dissemination on matters relating to violations of customs laws, and to a lesser extent, anti-narcotics law. The DRI maintains close liaison with all the important enforcement agencies and with the Customs and Central Excise Commissariats. It also maintains close liaison with the World Customs Organisation (WCO) in Brussels, the Regional Intelligence Liaison Office (RILO) in Tokyo, INTERPOL and foreign Customs Administrations.

97. The **National Crime Records Bureau (NCRB)**: The NCRB has been set up with the objective to empower the Indian police services with information technology and criminal intelligence in view of enabling them to effectively and efficiently enforce the law. It therefore creates and maintains secure sharable national databases on crimes, criminals, property and organised criminal gangs for use by law enforcement agencies. The NCRB processes and disseminates finger print records of criminals, including foreign criminals, to establish their identity.

98. The **State Police**: Under the Constitution of India, 'Police' and 'Public Order' are State subjects. Every State/Union Territory has its own police force, which performs not only normal policing duties but also has specialised units to combat terrorism in its various facets. The State Police also investigate and prosecute offenders for other offences, a number of which constitute predicate offences under the PMLA. The Central Government, through the MHA and its agencies, maintains close liaison with the State Police.

Financial Sector Agencies

99. In India, different segments of the financial system are regulated by different regulators. The Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority (IRDA) are the three major regulators. The National Housing Bank (NHB) is the sectoral regulator for housing finance companies while the Department of Economic Affairs within the Ministry of Finance is the regulator for some of the financial activities of India Post. The regulatory structure has evolved over a period of time parallel with the Indian financial system.

100. The **Reserve Bank of India (RBI)**: The RBI was established in 1935 in accordance with the provisions of the Reserve Bank of India Act and has its central office in Mumbai. The RBI is fully owned by the Government of India but has autonomy when exercising its functions. The RBI's affairs are governed by a central Board of Directors appointed by the Government of India.

101. While the RBI is essentially a monetary authority, its founding statute mandates it to be the manager of public debt of the Government of India and the banker to the Government. The RBI has also been entrusted with the work relating to banking regulation and supervision by a separate enactment in 1949, the Banking Regulation Act. The regulation over foreign exchange was acquired through the FERA that was later replaced with FEMA. Moreover, when the Payments and Settlement Systems Act, 2007 (PSSA) came into force, the RBI got the legislative authority to be the regulator and supervisor of the payment and settlement systems. While legitimate businesses are thus captured under the provisions of the FEMA and the PSSA and are now also subject to the provisions of the PMLA (see below), there exists a sizeable and demonstrated informal sector that is operating illegally. There is no authentic method to estimate the correct size and scope of the informal/Hawala/Hundi. It is illegal activity and the ED and the RBI take effective steps to identify the guilty persons and bring them to justice. However, there seems to be some disagreement among competent authorities (and also the private sector) regarding the size and scope of the informal/Hawala/Hundi sector and the nature of the problem as it relates specifically to ML and FT (see Section 3.11 of the report for more details).

102. As a result of amendments to the RBI Act over time, the regulatory powers of the RBI now also cover NBFCs and all-India financial institutions. The Government Securities Act, 2006 empowers the RBI to frame regulations as to the terms and conditions for the issue of government securities, the form in which they can be issued and other related issues. Under the RBI Act, the RBI has been entrusted with the responsibility of managing the country's foreign exchange reserves. Thus, the main functions of the RBI, as laid down in the statutes, are: issuing of currency; banker and fiscal agent to the Government, including the function of debt management; and banker to other banks.

103. As indicated above, the RBI is in charge of the regulation and supervision of India's banking system under the provisions of the Banking Regulation Act, governing all scheduled commercial banks. The NBFCs are subject to the provisions of the Companies Act and are also regulated and supervised by the RBI under the provisions of the RBI Act. The RRBs were created under the RRB Act and are regulated by the RBI but supervised by the NABARD, The Rural Co-operative Banks; State Co-operative Banks (StCBs); and the District Central Co-operative Banks (DCCBs) are also regulated by the RBI under the Banking Regulation Act (as applicable to co-operative societies) but are supervised by the NABARD. The NABARD's supervisory powers are as follows:

- a. inspection, systems study, and off-site surveillance of RRBs and co-operative banks (other than urban/primary co-operative banks), such as StCBs and DCCBs;
- b. inspection of State Co-operative Agriculture and Rural Development Banks (SCARDBs) and apex non-credit co-operative societies apex Weavers Societies, Marketing Federations, etc on a voluntary basis;

- c. providing recommendations to the RBI on opening of new branches by StCBs and RRBs; and administering the Credit Monitoring Arrangements in this kind of institutions.

104. The **Securities and Exchange Board of India (SEBI)**: The SEBI is a statutory body constituted under the SEBI Act and is the registering, supervisory and regulatory body for the securities sector. The primary functions of the SEBI consist of protecting the interests of investors in securities; promoting the development of the sector; and regulating the securities market for matters connected therewith. SEBI is also the regulator for related intermediaries, stock exchanges, depositories, credit rating agencies, foreign institutional investors (FIIs) and collective investment schemes, such as mutual funds.

105. The **Insurance Regulatory and Development Authority (IRDA)**: The opening up of the insurance sector in 1999 led to the setting up of a separate regulator for the insurance sector, the IRDA. The objectives of IRDA as laid down in its Mission Statement are “To protect the interests of the policy holders, and to regulate, promote and ensure orderly growth of the insurance industry and for matters connected therewith or incidental thereto”.

106. The **National Housing Bank (NHB)**: The housing finance companies are currently regulated and supervised by the National Housing Bank.

Financial sector bodies – Associations

107. The **Indian Banks' Association (IBA)**: The IBA was formed in 1946 as a voluntary association of banks in India with 22 members. At the time of the on-site visit, the IBA had 160 members comprising public sector banks, private sector banks, foreign banks having offices in India and urban co-operative banks. The role and responsibilities of the IBA are to promote and develop sound and progressive banking principles, practices and conventions in India and to contribute to the development of creative banking. The IBA also renders assistance in providing various common services to its members. It also develops and implements new ideas and innovations in banking services, operations and procedures and provides a platform for banks for co-ordination and co-operation on procedural, legal, regulatory, technical, administrative or operational problems in banking. The IBA is an associated member of the International Banking Federation.

108. The **Life Insurance Council (LIC)**: All life insurance companies are members of the LIC. The objective of the LIC is to play a significant and complementary role in transforming India's life insurance industry into a vibrant, trustworthy and profitable service. It assists in maintaining high standards of ethics and governance among the insurers. The LIC organises structured and pro-active discussions with Government, law makers and regulators and plays a leading role in insurance education, research, training and conferences.

109. The **Association of Merchant Bankers of India (AMBI)**: The AMBI was granted recognition by SEBI to set up professional standards for providing efficient services and establishing standard practices in merchant banking and financial services. The AMBI was promoted to exercise overall supervision over its members in the matters of compliance with statutory rules and regulations pertaining to merchant banking and other activities.

110. The **Association of Mutual Funds in India (AMFI)**: The AMFI, the body of all the registered Asset Management Companies, was incorporated in 1995 as a non-profit organisation. Its main function is to define and maintain high professional and ethical standards in all areas of operation of the mutual fund industry. It recommends and promotes best business practices and a code of conduct to be followed by members and others who are engaged in activities of mutual fund and asset management, including agencies connected or involved in the field of capital markets and financial services. The AMFI interacts

with the SEBI and promotes and implements a programme of training and certification for all intermediaries and other engaged in the industry.

111. The ***Foreign Exchange Dealers Association of India (FEDAI)***: The FEDAI was set up in 1958 as an association of banks dealing in foreign exchange in India. It is a self-regulatory body and its major activities include framing of rules governing the conduct of inter-bank foreign exchange business among banks and liaison with the RBI for reforms and development of the FOREX market. The number of members of the FEDAI at the time of the on-site visit was 90.

112. The ***FOREX Association of India***: The FOREX Association of India, affiliated to the "Association of Cambiste Internationale" based in Paris, is a national organisation whose members are actively involved in the foreign exchange trading and the foreign exchange risk management. The FOREX Association of India is a self-financing body that tries to ensure that markets are transparent and foreign exchange transactions are conducted in a professional manner. It is an informal forum for exchanging news and views on the latest developments on both financial and technological levels.

DNFBP and other matters

113. The ***Bar Council of India (BCI)***: The BCI is a statutory entity responsible for regulating the Indian legal profession.

114. The ***Institute of Company Secretaries of India (ICSI)***: The ICSI exercises professional supervision over the members of the Institute who are in practice and tries to ensure adherence to professional ethics and code of conduct.

115. The ***Institute of Chartered Accountants of India (ICAI)***: The ICAI regulates the profession of Chartered Accountants in India. Its focus is on education, professional development, issuance and maintenance of high accounting, auditing and ethical standards along with overall regulatory function, including disciplinary mechanism. ICAI is the second largest professional body for accountants in the world.

Registries and Bodies Governing Legal Arrangements

116. The ***Registrar of Companies (ROC)***: The ROC is the Registry for companies and limited liability firms and is established under the MCA. The MCA has a three-tier organisational set-up namely, the Secretariat in New Delhi, the Regional Directorates in Mumbai, Kolkata, Chennai and Noida, and offices of the ROC in all States and Union Territories.

117. The ***Registrar of Societies (ROS)***: The ROS for non-profit societies is within State Government's purview and most of the States have an office of ROS. The Society Registration Act is a central Act but many States have adopted the Act with some State amendments, and are registering non-profit societies under their respective Act. Some State Governments have enacted completely separate legislation on the subject. The majority of NPOs are incorporated as a society and are registered with the ROS.

c. Approach concerning risk

118. As indicated above, India has undertaken risk assessments which led to amendments to the UAPA and the establishment of the NIA in 2008 and amendments to the PMLA in 2009. Moreover, with respect to other threats, such as drug trafficking, counterfeiting of currency, transnational crime, etc., various inter-ministerial committees/groups are in place to review these threats and to suggest appropriate counter-measures. An inter-ministerial committee consisting of members from the concerned ministries, the law enforcement agencies and the FIU-IND conducted a risk assessment of DNFBPs (see Section 4 of this report).

119. India has also adopted a risk-based approach in developing and implementing its AML/CFT regime by issuing Rules under the PMLA (the PML Rules) that suggest some minimum requirements to be respected. Discretion has been granted to the financial regulators to formulate and implement client identification programmes subject to minimum requirements and other additional requirements that they consider appropriate to mitigate the risk perceived for a particular type of client, product or service. Circulars issued by the relevant regulators provide examples of low risk customers to whom financial institutions may apply simplified measures. Moreover, financial institutions are required to apply enhanced CDD measures to customers estimated to be high risk. This approach implies that the financial institution must conduct a risk assessment to determine whether a customer is high or low risk (see also Section 3 of this report).

d. Progress since the last mutual evaluation

120. The current mutual evaluation of India is India's first mutual evaluation by the FATF. However, as a member of the APG, India was subject to a mutual evaluation in 2005 (based on the AML/CFT Methodology 2004) and the Mutual Evaluation Report (MER) was adopted by the APG Plenary in 2006. India has taken steps to address some of the deficiencies identified in its first MER. The most important changes in India's AML/CFT regime since 2005 are summarised below:

Criminalisation of money laundering

121. The PMLA came first into force in July 2005. The amendments to the PMLA enacted in 2009 were meant to better meet the requirements of the Vienna and Palermo Conventions. The range of offences in both Part A (offences without threshold) and Part B (offences with an INR 3 million/USD 60 000¹² threshold) of the Schedule of predicate offences was expanded and a new Part C "Offences with cross border implications" without threshold limit has been added to the Schedule of predicate offences.

Criminalisation of terrorist financing

122. The UAPA was amended in December 2008 to change the scope of the provision of funds, to ensure a broader coverage of the FT offence, and to change the definition of property in an effort to bring the legislation more in line with the requirements of the United Nations Convention for the Suppression of the Financing of Terrorism.

Confiscation, freezing and seizing of proceeds of crime

123. The PMLA was amended in 2009 and now allows proceeds of crime to be seized and confiscated regardless of whose possession they are in.

Freezing of funds used for terrorist financing

124. The UAPA was amended in December 2008 and a new section 51A has been inserted to give effect to the UNSCRs 1267 and 1373 and to complete its administrative freezing system. Subsequent to the amendment of the UAPA in December 2008, the Central Government (MHA) has issued on 27 August 2009 instructions and guidance in the form of an Order laying down the procedure for freezing, seizing, and attaching of assets under section 51A of the UAPA.

The Financial Intelligence Unit and its functions

125. The Financial Intelligence Unit-India (FIU-IND) has been set up as the "central national agency for receiving, processing, analysing and disseminating information relating to suspect financial transactions". The FIU-IND became fully operational in March 2006 and received on the average around

¹² Conversion rate throughout the report, which reflects the conversion rate at the time of the on-site visit: 50 INR = 1 USD.

500 000 Cash Transaction Reports (CTRs) and around 600 Suspicious Transaction Reports (STRs) every month in 2009. The FIU joined the Egmont Group as a member in May 2007 and regularly exchanges information with foreign FIUs.

Law enforcement, prosecution and other competent authorities

126. India has notified various Rules for effective implementation of the PMLA. India is a Federation and maintenance of law and order is within the domain of Provincial/State Governments. Considering the special nature of the money laundering offence, the enforcement of the PMLA has been kept with the Central Government. By notifications, the Directors of the FIU-IND and the Directorate of Enforcement have been conferred powers to enforce the Act and discharge other functions. An Adjudicating Authority has been appointed and an Appellate Tribunal has been constituted. By various notifications, 52 courts of sessions have been designated as Special Courts under the provisions of the PMLA. India has also started efforts to maintain a central database to enable review of the effectiveness of its AML/CFT provisions.

Risk of money laundering or terrorist financing

127. The authorities have not undertaken a single risk assessment of all the financial institutions operating in India, but some assessments have been completed for individual sectors. Various inter-ministerial committees and groups, under the umbrella of the Ministries of Finance and Home Affairs, are in place to review the threats, vulnerabilities and risks in different parts of the financial sector. These reviews have not resulted in any decisions to exclude specific institutions or types of activity from the AML/CFT regime on the basis that they pose a low or negligible risk for ML/FT purposes.

Customer due diligence, including enhanced or reduced measures

128. The PMLA Rules came into force in July 2005 to introduce a range of high-level obligations, and were subsequently strengthened in November 2009 and February 2010. In addition, the individual regulatory authorities (RBI, SEBI and IRDA) have issued their own circulars (considered to be “other enforceable means” – see Section 3 of the report), which require the implementation of much of the detail required under the FATF standard. However, there has been only a limited attempt to standardise the circulars, with the result that there are marginal variations in the obligations imposed on different sectors. Currently, there is a range of circulars, all of which have similar messages, but which contain different language and impose marginally different obligations. While some of these differences are entirely reasonable to reflect the different nature of the businesses, others seem simply to reflect different drafting styles or minor variations on a theme adopted by the individual agencies or departments.

Record-keeping, wire transfers and monitoring of transactions

129. The PMLA and the PMLA Rules as they existed until 12 February 2010, have several gaps in complying with the requirements of Recommendation 10. Although the 12 February 2010 amendments (exactly within the two month deadline after the on-site visit) corrected several though not all technical deficiencies, the gap in the record-keeping requirements preceding that date would necessarily have had significant negative impact on the effective implementation of record-keeping requirements meeting the FATF standard. The RBI, SEBI and IRDA have issued detailed circulars in view of ensuring compliance with the record-keeping and wire transfer rules and monitoring of transactions. It should be noted, however, that the remaining technical shortcomings with regard to Recommendation 10 cannot be addressed by these circulars, which are to be considered as other enforceable means.

Suspicious transaction reports and other reporting

130. The reporting requirements under the PMLA, accompanying Rules and circulars issued by the RBI, SEBI and IRDA impose statutory obligations on financial service providers to report STRs to the FIU-IND within a prescribed time. The regulators have clarified that all attempted transactions must be reported

in STRs, even if not completed by customers, irrespective of the amount of the transaction. After the amendment of the PMLA in 2009, FT offences became predicate offences under the PMLA and the STR reporting requirement also extends to terrorist financing. Since the amendments to the Rules framed under the PMLA in May 2007, the definition of “suspicious transaction” includes transactions which give rise to a reasonable ground of suspicion that they may involve financing of activities relating to terrorism”. The amendments to the Rules in November 2009 outline that suspicious transactions need to be reported regardless of the amount involved. In addition, the client verification requirements have been strengthened and the Rules now also prohibit financial institutions from keeping anonymous accounts. MVTS and Money Changers have been brought within the reporting ambit of PMLA in 2009. Since the PMLA came into force, the reporting entities are also required to report CTRs.

Internal controls, compliance, audit and foreign branches

131. The PMLA Rules and regulatory guidelines (circulars) issued by RBI, SEBI and IRDA stipulate that covered institutions must have appropriate systems and controls to comply with their obligations under the Act. The respective regulators have published specific instructions (in the form of regulatory guidelines/circulars) that are tailored to the needs of each of the sectors covered by the PMLA. Besides reference to the general control environment, some (but not all) of these instructions include requirements to have a specific AML compliance function, to put in place an ongoing staff training programme, and to have procedures for effective screening of potential employees. Financial institutions that operate overseas branches or subsidiaries have been advised to implement whichever is the more rigorous of either the Indian or the host country AML obligations.

The supervisory and oversight system - competent authorities and SROs

132. Under the PMLA, Rules and regulatory guidelines, India has foreseen a specific role and powers for the regulatory authorities (RBI, SEBI and IRDA) and the FIU-IND to explicitly monitor covered institutions’ compliance with the AML/CFT obligations. The RBI, SEBI and IRDA have regulatory powers and supervisory capacity and these now also include ensuring compliance with the AML/CFT provisions as part of their inspection and auditing process. It should be noted, however, that the component of the supervisory system focusing on AML/CFT is relatively new and not yet fully implemented.

AML/CFT Guidelines

133. The RBI, SEBI and IRDA have issued circulars to the institutions under their supervision to comply with the provisions in the PMLA and the corresponding Rules. The IBA has also issued and recently updated its guidance paper for banks. In addition, interaction between the FIU-IND, the regulators and the principal officers of the most important reporting entities takes place on a regular basis to review the institutions’ compliance with the AML/CFT obligations and to provide feedback.

Preventive Measures Designated Non-Financial Businesses and Professions

134. Following the amendments to the PMLA in 2009, casinos have been made subject to the KYC, CDD and reporting obligations in the PMLA. None of the other DNFBP sectors has been brought within the AML/CFT framework. The FIU-IND has initiated interaction with the various professional bodies such as the Bar Council of India, the Institute of Chartered Accountants of India, the Institute of Cost and Works Accountants of India since January 2008 to draw their attention to AML/CFT issues and the vulnerabilities of these sectors in this regard. An inter-ministerial committee was constituted by the Government in 2009 to conduct a risk assessment of DNFBP sectors and to suggest mechanisms to address the risks in consultation with the respective sector regulators.

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 *Criminalisation of Money Laundering (R.1 & 2)*

2.1.1 *Description and Analysis*

Recommendation 1

135. India has criminalised money laundering (ML) under both the Prevention of Money Laundering Act, 2002 (PMLA) as amended in 2005 and 2009, and the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act) as amended in 2001. While the ML provisions under the NDPS Act only relate to predicate drug offences, the PMLA applies to a much broader range of predicate offences, including narcotics.

136. The relevant provisions are as follows:

PMLA

Section 3: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

NDPS Act

Section 68C: "Prohibition of holding illegally acquired property.

(1) ... it shall not be lawful for any person to whom this Chapter applies to hold any illegally acquired property either by himself or through any other person on his behalf".

Section 8A. Prohibition of certain activities relating to property derived from offence.

No person shall

(a) convert or transfer any property knowingly that such property is derived from an offence committed under this Act or any other corresponding law of any country or from an act of participation in such offence, for the purpose of concealing or disguising the illicit origin of the property or to assist any person in the commission of an offence or to evade the legal consequences; or

(b) conceal or disguise the true nature, source, location, disposition of any property knowing that such property is derived from an offence committed under this Act or under any other corresponding law of any other country; or

(c) knowingly acquire, possess or use any property which was derived from an offence committed under this Act or under any other corresponding law of any other country."

Consistency with the United Nations Conventions

137. The Vienna and Palermo Conventions require countries to establish a criminal offence for the following knowing/intentional acts: conversion or transfer of proceeds for specific purposes; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and - subject to the fundamental/constitutional principles or basic concepts of the country's legal system - the sole acquisition, possession or use of proceeds (Art. 3(1)(b)&(c) of the Vienna Convention; and Art. 6(1) of the Palermo Convention against Transnational Organised Crime – the TOC Convention).

138. Section 8A of the NDPS Act offence is an almost faithful transposition of the Vienna Convention ML provisions. The PMLA takes a different approach by using a terminology that by its broad wording is intended to generally correspond with the criminal activity targeted by both the Vienna and Palermo Conventions.

139. As said, the PMLA (s.3) provides that money laundering is committed where someone “directly or indirectly attempts to indulge, knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property”. The section 3 *mens rea* threshold is lower than the Art. 6.1(a) of the TOC Convention in that no specific purpose or intention is required. The substantive element of “projecting it as untainted property” carries the notion of knowing disguise, as required by the Conventions, but does not appear to cover all concealment activity, such as the physical hiding of the assets.

140. As for the “knowledge” mental element of the offence of money laundering required by the Conventions, this is satisfied in both the NDPS Act and the PMLA.

Definition of proceeds

141. The ML offence in the PMLA extends to any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence (see *infra* under the heading *predicate offences*) or the value of any such property (PMLA s.2(1)(u) - definition of proceeds of crime). Property is defined as any property or assets of every description, whether corporeal or incorporeal, moveable or immovable, tangible or intangible and includes deeds and instruments evidencing title to, or interest in, such property or assets, wherever located (PMLA s.2(1)(v)).

142. Since the NDPS Act does not contain any general definition of property or proceeds of crime, the relevant definitions in the Code of Criminal Procedure (CrPC) apply. Similarly to the PMLA definitions, the term proceeds of crime means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity (including crime involving currency transfers) or the value of any such property (CrPC s.105A(c)); while the term property means property and assets of every description whether corporeal or incorporeal, moveable or immovable, tangible or intangible and deeds and instruments evidencing title to, or interest in, such property or assets derived or used in the commission of an offence and includes property obtained through proceeds of crime (CrPC s.105A(d)).

143. It is no formal and express legal condition that a conviction for the predicate offence is required as a precondition to prosecute money laundering, although some practitioners the assessment team met with felt that only a conviction would satisfactorily meet the evidentiary requirements. The definition of property in the PMLA (see *supra*) however requires property to be “related to a scheduled offence”. Consequently, the section 3 ML offence not being an “all crimes” offence, in the absence of case law, it is generally interpreted as requiring at the very minimum positive proof of the specific predicate offence before a conviction for money laundering can be obtained, be it for third party or self-laundering.

144. Similarly, under section 8A of the NDPS Act, although it is debatable that the person charged with money laundering needs to have been convicted of a predicate offence, the positive and formal proof of a nexus with a drug-related predicate offence is essential.

Predicate offences

145. As far as the PMLA is concerned, India follows the list approach for predicate offences according to the Schedule to the PMLA, as amended by the Prevention of Money Laundering (Amendment) Act since 1 June 2009. The Schedule comprises three Parts:

- a. Part A covering 33 offences without threshold value;

- b. Part B covering 46 offences with a threshold value of INR 3 million (“30 lakh rupees”) or USD 60 000;
- c. Part C including all offences listed in Part A and Part B (without monetary threshold), supplemented by all offences covered by Chapter XVII of the Indian Penal Code, 1860 (IPC - offences against property), when these offences have cross-border implications.

All in all, the list of predicate offences includes 156 offences under 28 different statutes.

146. According to section 2(v)(ra) of the Prevention of Money Laundering (Amendment) Act, 2009 an offence with cross border implications that is included in Part C of the Schedule means:

- a. any conduct by a person at a place outside India which constitutes an offence at that place and which would have constituted an offence specified in Part A, Part B or Part C of the Schedule, had it been committed in India and if such person remits the proceeds of such conduct or part thereof to India; or
- b. any offence specified in Part A, Part B or Part C of the Schedule which has been committed in India and the proceeds of crime, or part thereof have been transferred to a place outside India or any attempt has been made to transfer the proceeds of crime, or part thereof from India to a place outside India.

So only since the 2009 Amendment, predicate offences for money laundering also 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.

147. Although the scheduled offences now include a range of offences in each of the designated categories of offences, all offences under Schedule B only count as a predicate to money laundering where the value involved is INR 3 million/USD 60 000 or more.

Table: Designated categories of offences with schedule offences under the PMLA

| | Designated category of offence | Name of Act in the Schedule of PMLA |
|---|--|---|
| 1 | Participation in an organised criminal group and racketeering | Indian Penal Code, 1986 (s.120B - criminal conspiracy) – Part B of the Schedule |
| 2 | Terrorism, including terrorist financing | The Unlawful Activities (Prevention) Act, 1967 (ss.10 read with section 3; 11 read with ss.3 and 7; 13 read with s.3, 16 read with s.15, 16A, 17,18,18 A,18 B,19, 20 ,21, 38, 39 and 40) – Part A of the Schedule |
| 3 | Trafficking in human beings and migrant smuggling | The Bonded Labour System (Abolition) Act, 1976 (ss. 16, 18 and 20) – Part B of the Schedule The Transplantation of Human Organs Act, 1994 (ss.18, 19 and 20) – Part B of the Schedule The Child Labour (Prohibition and Regulation) Act, 1986 (s.14) – Part B of the Schedule The Juvenile Justice (Care and Protection of Children) Act, 2000 (ss.23 to 26) – Part B of the Schedule The Emigration Act, 1983 (s.24) – Part B of the Schedule The Passport Act, 1967 (s.12) – Part B of the Schedule The Foreigners Act, 1946 (ss.14, 14B and 14C) – Part B of the Schedule |
| 4 | Sexual exploitation, including sexual exploitation of children | The Immoral Traffic (Prevention) Act, 1956 (ss.5, 6, 8 and 9) – Part B of the Schedule |

| | Designated category of offence | Name of Act in the Schedule of PMLA |
|----|---|--|
| 5 | Illicit trafficking in narcotic drugs and psychotropic substances | The Narcotic Drugs and Psychotropic Substances Act, 1985 (ss15 to 24, 25A, 27A and 29) – Part A of the Schedule |
| 6 | Illicit arms trafficking | The Arms Act, 1959 (ss. 25 to 30) – Part B of the Schedule |
| 7 | Illicit trafficking in stolen and other goods | The Indian Penal Code, 1860 (ss.411 to 414) – Part B of the Schedule |
| 8 | Corruption and bribery | The Prevention of Corruption Act, 1988 (ss.7 to 10 and 13) – Part B of the Schedule |
| 9 | Fraud | The Indian Penal Code, 1860, (ss.417 to 424) – Part B of the Schedule |
| 10 | Counterfeiting currency | The Indian Penal Code, 1860 (ss.489A and 489B) – Part A of the Schedule |
| 11 | Counterfeiting and piracy of products | The Copyright Act, 1957 (ss. 7 to 10 and 13) – Part B of the Schedule The Trade Marks Act, 1999 (ss.103, 104, 105, 107 and 120) – Part B of the Schedule The Information Technology Act, 2000 (ss.72 and 75) – Part B of the Schedule The Biological Diversity Act, 2002 (s.55 read with s.6) – Part B of the Schedule The Protection of Plant Varieties and Farmers' Rights Act, 2001 (ss.70 to 73 read with s.68) – Part B of the Schedule The Indian Penal Code, 1860 (s.255, 257 to 260, 475, 476, 486 to 488) – Part B of the Schedule |
| 12 | Environmental crime | The Environment Protection Act, 1986 (ss.5 read with section 7 and 8) – Part B of the Schedule The Water (Prevention and Control of Pollution) Act, 1974 (ss.41(2) and 43) – Part B of the Schedule The Air (Prevention and Control of Pollution) Act, 1981 (s.37) – Part B of the Schedule The Wild Life (Protection) Act, 1972 (s.51 read with ss.9, 17A, 39, 44, 48 and 49B) – Part B of the Schedule |
| 13 | Murder, grievous bodily injury | The Indian Penal Code, 1860 (ss.302, 304, 307, 308, 327, 329) – Part B of the Schedule |
| 14 | Kidnapping, illegal restraint and hostage-taking | The Indian Penal Code, 1860 (s.364A) – Part B of the Schedule |
| 15 | Robbery or theft | The Indian Penal Code, 1860 (ss.392 to 402) – Part B of the Schedule |
| 16 | Smuggling | The Customs Act, 1962 (s.135) – Part B of the Schedule |
| 17 | Extortion | The Indian Penal Code, 1860 (ss.384 to 389) – Part B of the schedule |
| 18 | Forgery | The Indian Penal Code, 1860 (ss.467, 471 to 473) – Part B of the Schedule |
| 19 | Piracy | The Suppression of Unlawful Acts against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002 (s.3) – Part B of the Schedule |
| 20 | Insider trading and market manipulation | The Securities and Exchange Board of India Act, 1992 (s.12A read with s.24) – Part B of the Schedule |

148. The predicate offences relating to money laundering in the NDPS Act only extend to the drug offences under the Act. The ML offence in this Act does specifically refer to drug offences that occurred in another country, provided that it would have constituted an offence had it occurred in India (NDPS Act s.8A(c)). Although not formally repealed, section 8A NDPS Act has become somewhat redundant with the introduction of the PMLA (Schedule A - drug related predicate offences) imposing much stiffer sanctions. On the other hand, unlike the PMLA, the ML definition under the NDPS Act fully corresponds with that of the Conventions.

Self-laundering

149. The PMLA money laundering offence applies to “*whoever*”, a term that includes the person who commits the predicate offence, if that person is knowingly involved in the laundering of the proceeds of his

crime. The NDPS Act ML provision simply refers to “no person”, without exception. Furthermore, no legal principle in India prevents the application of the ML provisions to the predicate offender.

Ancillary offences

150. Section 3 of the PMLA is construed in such way to encompass, beside the actual dealing with criminal proceeds, any attempt, assistance, being a party and actual involvement in a ML process or activity, and as such it generally covers all relevant ancillary offences, including – although not expressly stated - conspiracy. Criminal conspiracy as provided in sections 120A and B of the IPC and abetment as in section 107 of the PC apply to the PMLA offences anyway. The NDPS Act specifically provides for abetment and conspiracy in its section 29. Preparatory acts and attempts are covered by section 30.

Additional elements

151. India assumes extraterritorial jurisdiction where the proceeds of crime are derived from conduct by an Indian citizen that occurred in another country (IPC s.4). This is so even if the conduct is not an offence in that country but constitutes a predicate offence had it occurred domestically, on the condition it is one of the offences listed in one of the three parts of the Schedule to the PMLA.

Recommendation 2

Scope of liability

152. The offence of money laundering applies to *whosoever* (PMLA s.3), which in its generality covers any person. The PMLA defines “person” as “an individual” and all forms of companies, firms, associations and legal persons (PMLA s.2(s)). The NDPS Act (s.8A) refers to “No person ...”, which term is defined in the applicable General Clauses Act (s.3) as to include – beside the natural person - any company or association or body of individuals, whether incorporated or not.

153. The sanctions for money laundering under the PMLA are “rigorous” (*i.e.* with hard labour) imprisonment for three to seven years and a fine of up to INR 500 000 (USD 10 000). ML predicated by Schedule Part A, par. 2, narcotic offences carries a higher maximum penalty, namely 10 years imprisonment. On the other hand, where the ML offence relates to a drug offence under the NDPS Act, it comes under the general sanction provision in its section 32, which imposes a standard penalty for all offences in the Act which do not have a sanction specified, as is the case with section 8A. Consequently, the maximum penalty for money laundering under the NDPS Act is only six months, regardless of the amount laundered.

154. Legal persons are liable to be fined up to INR 500 000 (10 000 USD) under the PMLA (s.4). Violation of section 8A of the NDPS Act by a legal person is punished with an undefined fine (s.32), the amount of which is left to the sovereign appreciation of the court.

155. Section 70 of the PMLA and section 38 of the NDPS Act provide that where the violation of the Act is committed by a company, both the company and the individuals in charge of the company will be deemed to be guilty of that contravention unless they did not have the knowledge of contravention or they have exercised all due diligence to prevent it.

156. While the legal person is liable to be punished with a fine, imprisonment can obviously be imposed only on the natural persons in charge of and responsible for the “conduct” of the company¹³. The

¹³ In its judgement dated 24 February 2006 with respect to Civil Appeal No 1748, 1999 (*Standard Chartered Bank & Others Vs Directorate of Enforcement*) the Supreme Court stated that when a contravention is made by a company, “*the company as a person is liable to be proceeded against though in criminal prosecution the punishment by way of imprisonment can be imposed only on the officers of the company*”.

combination of penalty provisions (PMLA s.4/NDPS Act s.32) with the company provisions of section 70 of the PMLA/section 38 of the NDPS Act is interpreted by some prosecutors in the sense that no charges can be brought against a company without concurrently prosecuting the responsible natural person for the ML offence.

157. Parallel or additional proceedings can be initiated under other relevant statutes against a legal person being prosecuted under the PMLA. First of all, the assets of the company are liable to confiscation. Section 388B of the Companies Act provides for the possibility of destitution of managerial personnel of a company for indulging in *e.g.* fraudulent practices and money laundering that is found to have indulged in fraud etc. and against which company prosecution proceedings under relevant statutes including PMLA are likely to be initiated upon conclusion of investigations. Section 433 of the Companies Act provides for the dissolution of a company by the court. Also, licences of (financial) institutions can be revoked (see for instance s.10(3) of the FEMA).

158. It is a principle of Indian law that the intentional element of an offence, including the ML offence, can be inferred from objective factual circumstances. Section 3 of the Indian Evidence Act, 1872 provides that a fact is said to be proved when, after considering the matters before it, the court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists. Both direct evidence and circumstantial evidence are admissible in the Indian system of jurisprudence, and the admissibility of inference from factual circumstances to prove the guilt of an offender has been confirmed by the Supreme Court in firm jurisprudence¹⁴.

Recommendation 30 – Resources of prosecutorial authorities

159. The Principal Law Officer of the State is known as the Advocate-General. Each State Government has a Director of Prosecution responsible for making all arrangements for prosecution in all criminal cases. Senior Public Prosecutors, Special Public Prosecutors, and Public Prosecutor are advocates working on a retainer basis with experience in criminal cases. Assistant Public Prosecutors prosecute criminal cases in Courts of Judicial Magistrates. All prosecutors have a University Degree in Law and requisite minimum experience depending on their positions.

160. Under the provisions of section 43 of the PMLA, 26 Special Courts have been constituted by the Central Government for trial of offences punishable under section 4 of the Act.

161. Three seminars were organised for judicial officers at the National Judicial Academy in which over 60 Judges from various High Courts and more than 100 Judges of the level of Session Judge from various States participated. The Academy has also included a specialised module on money laundering in its training courses for sensitising the judges with regard to the process of investigation, seizure, attachment, confiscation of assets, and also prosecutions of persons and entities involved in ML offences. The Directorate of Enforcement (ED) provided the trainers for the training course.

Recommendation 32 - Statistics

162. The Director of Enforcement (ED) maintains statistics on ML investigations, prosecutions and convictions under the PMLA. The statistics below relate to the number of investigations and prosecutions

¹⁴ For instance, in its judgment dated 31 May 2007 with respect to Civil Appeal No 1254, 2006 *Manik Das and Ors. Vs. State of Assam*, the Supreme Court stated that “*direct proof of common intention is seldom available and, therefore, such intention can only be inferred from the circumstances appearing from the proved facts of the case and the proved circumstances*”.

for the ML offence between 2006 and the end of 2009. The important increase in the number of investigations in 2009 was explained as an effect of the 2009 amendment of the PMLA widening the scope of the scheduled predicate offences, particularly in respect of drug offences, and of the possibility for the ED to intervene at an earlier stage of the investigation process (see Section 2.6 below).

Statistics: Money Laundering cases

| | Items | Financial year 2006-2007 | Financial year 2007-2008 | Financial year 2008-2009 | Financial year 2009-2010 (31 December 2009) | Total |
|----|----------------------------|-----------------------------|-----------------------------|--------------------------------|---|-------|
| a. | No. of ECIRs | 27 | 15 | 17 | 739 | 798 |
| b. | No. of persons arrested | 7 | - | - | 9 | 16 |
| c. | No. of prosecutions filed. | - | - | 2 | 4 | 6 |

ECIR: Enforcement Case Information Report = number of investigations.

163. There have been no prosecutions for money laundering at all under the NDPS Act. Here the focus was on prosecuting the predicate drug offence itself and confiscating the proceeds.

Implementation and effectiveness

164. When the PMLA was enacted on 1 July 2005 implementing the Palermo TOC Convention, it was already clear that the scope of the law was too restrictive to withstand the test of the relevant international standards. With the extension of the list of predicate offences under Schedule A and B, and the addition of Schedule C offences since 1 June 2009, India has made a serious effort to bring the ML criminalisation of the PMLA in line with the FATF criteria in this respect. It did not do away with all shortcomings, however.

165. Firstly, it is not clear why the legislator abandoned the NDPS Act approach to define the ML activity by simply incorporating the relevant Convention language in the domestic law. With the section 3 of the PMLA money laundering provision, a newly defined ML offence was introduced differing from the comprehensive qualification of section 8A of the NDPS Act that was not repealed, resulting in the co-existence of two divergent drug related ML offences.

166. The new definition of the ML offence in section 3 of the PMLA tries to capture all requisite mental and physical elements of the Convention's ML provision in one overarching sentence. The *mens rea* element is the "knowledge" standard as minimally required by the Conventions. Section 3 of the PMLA does not require a specific intention or purpose, and as such its threshold is lower than that of Art. 6.1(a)(i) of the TOC Convention. The provision however falls short on the following *actus reus* aspects:

- a. The physical element in all cases includes the substantive condition of "*projecting (the proceeds of crime) as untainted property*", so although the broad formulation of "*any process or activity*" covers any conduct involving criminal proceeds, such conduct is only criminalised as money laundering when the property is concurrently projected as untainted. While this "projection" circumstance may correspond with the notion of "disguise" as in Art. 6.1(a)(ii) of the TOC Convention, it does not cover acts of physical concealment without any "projecting" (such as deposit in a safe), even if – as was argued - this act is seen as an attempt to "project", *quod non*.
- b. With the imposition of the "projecting" condition the PMLA offence does not extend to the activity of sole "acquisition, possession or use" of criminal proceeds as stated in Article 6(1)(b)(i) of the TOC Convention, although this would not be contrary to the basic concepts of the Indian legal system. Only the offences of "holding" drug proceeds (NDPS Act s.68C) or "proceeds of terrorism" (UAPA s.21) are unconditional and may be considered to cover

“possession” situations in these specific circumstances. Also, the sections 410 and 411 IPC “receiving” offence may cover acts of “acquisition”, but these provisions fall short in respect of the scope of predicate offences, as they only apply to stolen (or equivalent¹⁵) property.

167. A more serious, and in fact a major deficiency however are the restrictions that come with the predicate offences listed in Schedule Part B, as these offences carry a threshold of 3 million INR (USD 60 000) before they qualify as predicates, except if they have “cross-border implications” (Schedule Part C). So the 2009 Amendment to the PMLA did not satisfactorily address this deficiency that was already highlighted in the previous APG assessment. The authorities explained their perseverance to maintain the threshold condition by their concern not to overburden the law enforcement authority (the Directorate of Enforcement - ED), designated to pursue the financial and proceeds of crime aspects of the predicate offences, with the investigation of petty crimes, so they can concentrate on serious cases. Indeed, in practice targeted ML investigations by the ED are conducted concurrently with or consecutive to predicate offence enquiries by the State Police. Be that as it may, the threshold condition, even when mitigated by the cross-border exception, clearly goes against the FATF standard. Besides, the artificial differentiation between illegal and admissible activity solely based on the amounts involved does not find any justifiable objective grounds and negates the gravity of any money laundering activity as such. Moreover, it leaves a gap in the AML system that may negatively impact on effective prosecution and general deterrence.

168. The linkage and interaction of the ML offence with a specific predicate criminality is historically very tight in the Indian AML regime. The concept of stand-alone money laundering is quite strange to the practitioners, who cannot conceive pursuing money laundering as a *sui generis* autonomous offence. Some interlocutors were even of the (arguably erroneous) opinion that only a conviction for the predicate criminality would effectively satisfy the evidential requirements. As said, this attitude is largely due to the general practice in India to start a ML investigation only on the basis of a predicate offence case. Even if the ML investigation since recently can run concurrently with the predicate offence enquiry, there is no inter-agency MOU or arrangement to deal with evidentiary issues between the various agencies in investigating predicates and ML offences. Also, the way the interaction between the law enforcement agencies is presently structured carries the risk that ML prosecutions could be delayed while the other predicate offence investigation agencies try to secure convictions.

169. While the strict evidentiary standard in respect of the proof of the predicate offence - as interpreted by the law enforcement authorities in the absence of any jurisprudence on this issue - may be considered manageable when both the predicate and the laundering activity fall under the Indian jurisdiction, the proof of foreign predicates represents a far greater challenge. There may be an effectiveness issue as in that case the Indian law enforcement authorities are not in control and they are either dependent on the foreign jurisdiction supplying the formal and specific proof or they have to go out and conduct the investigations themselves.

170. Furthermore, although there is some disagreement between the practitioners on this point, the practice of making corporate criminal liability contingent on the prosecution of the natural person in charge of the company, gives rise to an effectiveness concern. This appears to be the result of an overly literal interpretation of section 4 of the PMLA and section 8A of the NDPS Act where they provide for both imprisonment and fines, and do not differentiate between legal or natural persons, although neither the submitted case law nor section 305 of the CrPC on the prosecution of corporations impose such rule¹⁶ This

¹⁵ “Stolen” property includes property derived from extortion, robbery, misappropriation or breach of trust (IPC s.410)

¹⁶ The cited jurisprudence of the Supreme Court (*Standard Chartered Bank & Others Vs Directorate of Enforcement*) confirms that imprisonment can only be imposed on “the officers” of the company, but does not actually say that you cannot prosecute one without the other. In *Kamal Goyal Vs United Phosphorus*

interpretation may indeed obstruct prosecution where the responsible individual cannot be identified or stays outside the jurisdiction of the courts¹⁷. One of the rationales behind the corporate criminal liability standard is precisely to enable independent law enforcement action against legal entities whenever such action is impossible against the natural persons involved or the criminally responsible individual cannot be identified.

171. While the sanctions under the PMLA may be considered to be effective, proportionate and dissuasive, this is not the case for the sanction for the drugs ML offence in the NDPS Act, particularly when large sums of money are laundered (imprisonment of 6 months and an undefined fine). The NDPS Act money laundering provision being outdated and overtaken by the PMLA, it is advisable to do away with this redundancy anyway.

172. The INR 500 000 (USD 10 000) maximum fine provided for legal persons for transgressions of the PMLA equally seems rather low, taking into account the possible scale of the ML activity and the financial capacity of most commercial companies.

173. All in all, there clearly is an effectiveness issue. The whole system is historically keyed to domestic situations, where both the predicate and the money laundering are under Indian jurisdiction and covered by the national law enforcement capacity. Before the introduction of the cross-border clause of Schedule Part C on 1 June 2009, foreign predicate offences did not even qualify legally as criminal activity underpinning ML activity in India. Whenever the predicate criminality is committed outside India, law enforcement is totally dependent on the formal and positive proof being supplied by the foreign jurisdiction or the Indian police must investigate the foreign predicate offence themselves to the satisfaction of the high evidentiary requirements, bearing in mind there is still no jurisprudential guidance on this important issue.

174. Effectiveness concerns are primarily raised by the total absence of any ML conviction, although the NDPS Act is already in effect since 2 October 2001 and the PMLA since 1 July 2005. At the time of the on-site visit only 6 prosecutions were underway, with the first proceedings starting in 2008. This also means case law yet has to be developed on the correct interpretation and implementation of the law, particularly on the evidentiary requirements. The Indian authorities expect a significant improvement in this regard now that (1) the mechanism for sharing of information between the Directorate of Enforcement and the LEAs investigating the scheduled offences has been institutionalised, and (2) the 2009 amendment of PMLA allows ML investigations to be initiated immediately after the registration of a predicate offence by the LEA, facilitating parallel and simultaneous investigations by the Directorate of Enforcement into the offence of money laundering.

2.1.2 Recommendations and Comments

175. Although recently an increased focus on the ML aspect and use of the ML provisions is to be acknowledged, there are still some important and often long-standing legal issues to be resolved. To that end following measures should be taken:

- The monetary threshold limitation of INR 3 million for the Schedule Part B predicate offences should be abolished.
- The section 3 PMLA definition of the ML offence should be brought in line with the Vienna and Palermo Conventions so as to also fully cover the physical concealment and the sole acquisition, possession and use of all relevant proceeds of crime.

the Delhi High Court quashed the criminal complaint against the accused individual, but ordered the trial court to proceed with the complaint as far as the company was concerned.

¹⁷ No *in absentia* proceedings are possible in India for ML or FT.

- The present strict and formalistic interpretation of the evidentiary requirements in respect of the proof of the predicate offence should be put to the test of the courts to develop case law and receive direction on this fundamental legal issue.
- The level of the maximum fine imposable on legal persons should be raised or left at the discretion of the court to ensure a more dissuasive effect.
- The practice of making a conviction of legal persons contingent on the concurrent prosecution/conviction of a (responsible) natural person should be abandoned.
- Consider the abolishment of the redundant section 8A NDPS Act drug-related ML offence or, if maintained, bring the sanctions at a level comparable to that of the PMLA offence.

2.1.3 Compliance with Recommendations 1 and 2

| | Rating | Summary of factors relevant to s.2.1 underlying overall rating |
|-----|--------|---|
| R.1 | PC | <ul style="list-style-type: none"> • (High) monetary threshold condition for most ML predicates. • ML provision does not cover physical concealment of criminal proceeds. • ML provision does not cover the sole knowing acquisition, possession and use of criminal proceeds. • Effectiveness issues: <ul style="list-style-type: none"> ○ the absence of any conviction for ML; ○ the high evidentiary standard untested before the courts, particularly in respect of the proof of the foreign predicate offence. |
| R.2 | LC | <ul style="list-style-type: none"> • Inadequate sanctions for legal persons committing the ML offence. • Effectiveness issues: <ul style="list-style-type: none"> ○ the total absence of ML convictions; ○ the interpretation of making corporate criminal liability contingent on prosecution of a natural person. |

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

Special Recommendation II

176. The relevant Acts regarding the criminalisation of terrorist financing are:

- a. the Unlawful Activities (Prevention) Act, 1967 (UAPA) as amended by the Unlawful Activities (Prevention) Amendment Act, 2004 and the Unlawful Activities (Prevention) Amendment Act, 2008;
- b. the National Investigation Agency Act, 2008 (NIA Act);
- c. the Code of Criminal Procedure, 1973 (CrPC).

The Unlawful Activities (Prevention) Act (UAPA)

177. The UAPA is India's legislation dealing with combating terrorism in all its facets, including terrorist financing. The relevant sections of the UAPA in relation to terrorist financing are:

| Section | Description of offence |
|---------|--|
| 2 | Definition section |
| 17 | Punishment for raising funds for a terrorist act |

| Section | Description of offence |
|---------|---|
| 21 | Punishment for holding proceeds of terrorism |
| 38 | Offence relating to membership of a terrorist organisation |
| 39 | Offence relating to support given to a terrorist organisation |
| 40 | Offence of raising fund for a terrorist organisation |

The National Investigation Agency Act (NIA Act)

178. The NIA Act has resulted in the establishment of a federal investigating agency known as the National Investigation Agency (NIA) for investigation and prosecution of offences under the Acts mentioned in the Schedule to this Act, which are:

- a. the Atomic Energy Act, 1962;
- b. the Unlawful Activities (Prevention) Act, 1967;
- c. the Anti-Hijacking Act, 1982;
- d. the Suppression of Unlawful Acts against Safety of Civil Aviation Act, 1982;
- e. the SAARC Convention (Suppression of Terrorism) Act, 1993;
- f. the Suppression of Unlawful Acts against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002;
- g. the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005; and offences under:
 - i. chapter VI of the Indian Penal Code (ss.121 to 130 (both inclusive));
 - ii. sections 489-A to 489-E (both inclusive) of the Indian Penal Code.

The Code of Criminal Procedure (CrPC)

179. The CrPC contains detailed procedures for trial of criminal cases. Under the CrPC, magistrates, courts and investigating officers derive powers to register FT cases and to arrest a person as well as powers to search, seize, attach and enforce attendance and record of statements of witnesses, etc.

Characteristics of the terrorist financing offences

180. India has signed the International Convention for the Suppression of the Financing of Terrorism (FT Convention) on 8 September 2000 and ratified it on 22 April 2003. India is also party to the treaties listed in the annex to the FT Convention. Terrorist Financing has been criminalised under the UAPA, as amended in 2004 and 2008.

181. The UAPA criminalises terrorist financing according to its sections 17 and 40:

- a. section 17 criminalises raising or collecting or providing funds or attempting to provide funds knowing that such funds are likely to be used by any person or persons to commit a terrorist act in following terms: *“Whoever, in India or in a foreign country, directly or indirectly, raises or collects funds or provides funds to any person or persons or attempts to provide funds to any person or persons, knowing that such funds are likely to be used by such person or persons to commit a terrorist act, notwithstanding whether such funds were actually used or not for commission of such act, shall be punishable with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine”*.
- b. section 40 of the UAPA criminalises raising of funds for “terrorist organisations” that are listed in the Schedule to the Act (UAPA s.2.1(m)): *“A person commits the offence of raising*

fund for a terrorist organisation, who, with intention to further the activity of a terrorist organisation, (a) invites another person to provide money or other property, and intends that it should be used, or has reasonable cause to suspect that it might be used, for the purposes of terrorism; or (b) receives money or other property, and intends that it should be used, or has reasonable cause to suspect that it might be used, for the purposes of terrorism; or (c) provides money or other property, and knows, or has reasonable cause to suspect, that it would or might be used for the purposes of terrorism. A person, who commits the offence of raising fund for a terrorist organisation under sub-section (1), shall be punishable with imprisonment for a term not exceeding fourteen years, or with fine, or with both”.

182. The overarching condition of section 40 of the UAPA is the intent to further the activity of a terrorist organisation, whenever the suspect performs the (financing) activity of inviting to provide, receiving or providing funds for terrorism purposes.

183. It should be noted that terrorist acts (s.17) and terrorism (s.40) are synonymous terms. Also, there is no definition for the term “terrorist”, but it should be interpreted according to the meaning of “terrorist act” as in section 15 of the UAPA (UAPA s.2(k)). Furthermore, the application of section 40 of the UAPA is specifically limited to these organisations that are listed in the Schedule to the UAPA, i.e. S/RES/1267(1999) and the domestic terrorist organisations list, established according to chapter VI of the UAPA. Financing of other terrorist organisations or groups is deemed to be covered by the general section 17 provisions, where it refers to the term “person or persons”, which includes any “*association or body of individuals*” (General Clauses Act s.3).

184. According to Article 2 of the FT Convention the financing should pertain to 1) all offences covered by the 9 Treaties annexed to the Convention and 2) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act.

185. In order to comply with this Convention requirement, India has defined and listed the terrorist acts in section 15 of the UAPA as follows:

“Whoever does any act with intent to threaten or likely to threaten the unity, integrity, security or sovereignty of India or with intent to strike terror or likely to strike terror in the people or any section of the people in India or in any foreign country,

(a) by using bombs, dynamite or other explosive substances or inflammable substances or firearms or other lethal weapons or poisonous or noxious gases or other chemicals or by any other substances (whether biological radioactive, nuclear or otherwise) of a hazardous nature or by any other means of whatever nature to cause or likely to cause

(i) death of, or injuries to, any person or persons; or

(ii) loss of, or damage to, or destruction of, property; or

(iii) disruption of any supplies or services essential to the life of the community in India or in any foreign country; or

(iv) damage or destruction of any property in India or in a foreign country used or intended to be used for the defence of India or in connection with any other purposes of the Government of India, any State Government or any of their agencies; or (b) overawes by means of criminal force or the show of criminal force or attempts to do so or causes death of any public functionary or attempts to cause death of any public functionary; or

(b) overawes by means of criminal force or the show of criminal force or attempts to do so or causes death of any public functionary or attempts to cause death of any public functionary; or

(c) detains, kidnaps or abducts any person and threatens to kill or injure such person or does any other act in order to compel the Government of India, any State Government or the Government of a foreign country or any other person to do or abstain from doing any act, commits a terrorist act”.

186. The standards further require that the offence should extend to persons who collect or provide funds (a) with the *intention* that they be used for terrorism; or (b) in the *knowledge* that they are to be used for terrorism. Section 17 does not require a specific intention, but refers to persons who provide or collect or raise funds *knowing* that such funds are *likely* to be used to commit a terrorist act, so the knowledge of the mere possibility of such use suffices, and it does not matter whether such funds were actually used or not for the commission of such act. So the section 17 standard is low and satisfactorily covers the mental element of knowledge.

187. The section 40 offence of raising funds for a terrorist organisation refers to both an intentional and a knowledge mental element. It requires the intention of furthering the activity of the terrorist organisation, besides having the knowledge or a reasonable cause to suspect the funds could be used for terrorist purposes. In this respect however the international standards only require the intention or knowledge that the funds should or are to be used by a terrorist organisation, without any further condition of specific intention or purpose (see par. 3 of the Interpretative Note to SR.II).

Definition of “funds”

188. The UAPA does not define the term “funds”, but contains a definition of “property” that mirrors the definition of funds in Art. 1 of the FT Convention (UAPA s.2(1)(h)), with the addition of “cash and bank account”. The FT Convention ‘funds’ definition includes all forms of “property”, and in that sense these terms may be considered synonymous. The list of assets in the UAPA definition is exhaustive (“... *title to, or interest in, such property or assets by means of ...*”) and as such slightly deviates from the illustrative approach of Art. 1.1 of the FT Convention (“*assets including, but not limited to*”). With the added wording in s.2(1)(h), however, the definition seems to adequately cover all relevant assets. While defining property, the UAPA does not make a distinction between the legitimate or illegitimate origin of the property (“*however acquired*”).

189. Section 17 of the UAPA expressly states that it is irrelevant whether the funds were actually used for the commission of terrorist acts or not, nor is it necessary that the offence of raising or providing or collection of funds be linked to a particular terrorist act. Section 17 only requires knowledge that such funds are likely to be used by the beneficiary to commit a terrorist act. However, this specific knowledge condition excludes the situation where the donor/provider intends the funds to be used or knows they will be used for non-terrorist purposes, such as family support or personal comfort expenses.

Ancillary offences

190. As the section 511 of the IPC attempt provision exclusively applies to activity criminalised by the IPC, punishment for attempting FT should be specifically provided for in the UAPA. An attempt to provide funds to terrorists or terrorist groups (“person or persons”) is clearly criminalised in section 17 of the UAPA. The attempt however does not apply to acts of raising or collecting such funds. The section 40 terrorist organisations financing provision itself does not cover attempt situations. It was argued that section 18 of the UAPA sets out the offences for conspiracy, attempt, abetting, advising, inciting or knowingly facilitating the commission of a terrorist act or any act preparatory to the commission of a terrorist act, where terrorist financing would then fall within this last category. Finally, similar to the

ancillary offences for money laundering, conspiracy to commit an offence of terrorist financing can be covered by sections 120A and 120B of the IPC (criminal conspiracy) and chapter V of the IPC (abetting)

Predicate offences for money laundering and extraterritorial jurisdiction

191. As indicated in section 2.1 above, the PMLA has been amended with effect from 1 June 2009, and the Part A offences of the Schedule (offences without any threshold) now include the following offences under the UAPA:

| Section | Description of offence |
|--------------------------|--|
| 10 read with s.3 | Penalty for being member of an unlawful association, etc. |
| 11 read with ss. 3 and 7 | Penalty for dealing with funds of an unlawful association |
| 13 read with s.3 | Punishment for unlawful activities |
| 16 read with s.15 | Punishment for a terrorist act |
| 16A | Punishment for making demands of radioactive substances, devices, etc. |
| 17 | Punishment for raising fund for a terrorist act |
| 18 | Punishment for conspiracy, etc. |
| 18A | Punishment for organising of terrorist camps |
| 18B | Punishment for recruiting of any person or persons for a terrorist act |
| 19 | Punishment for harbouring, etc. |
| 20 | Punishment for being member of a terrorist gang or organisation |
| 21 | Punishment for holding proceeds of terrorism |
| 38 | Offence relating to membership of a terrorist organisation |
| 39 | Offence relating to support given to a terrorist organisation |
| 40 | Offence of raising fund for a terrorist organisation |

192. Beside establishing jurisdiction over the whole Indian territory, the UAPA extends the ambit of the Act to any person who commits an offence beyond India that is punishable under the Act, citizens of India who are outside India, Indian government officers wherever they are, and persons on Indian registered ships and aircrafts wherever they are (UAPA ss.(4) and (5)). The location of the terrorist organisation or terrorist activity is totally irrelevant in the context of section 17. India assumes universal jurisdiction over any FT activity as defined in section 17, wherever it occurs (“in India or in a foreign country”). Moreover section 15, which establishes the offence of a terrorist act, includes circumstances where a foreign country is threatened or terrorised. It is therefore not necessary for the person who committed the FT offence to be in the same country as the one in which the terrorist is located or the terrorist act occurred, for the UAPA to apply, as long as India has jurisdiction over the FT offence.

Scope of liability and sanctions

193. As with money laundering, the Indian jurisprudence allows the intentional element of an offence to be inferred from the objective factual circumstances (see Section 2.1 above).

194. In the absence of a definition in the UAPA, the General Clauses Act (s.3) applies, defining “person” to include legal persons (“*any company or association or body of individuals, whether incorporated or not*”), so criminal liability for terrorist financing extends to legal persons.

195. Penalties under the UAPA include imprisonment from five years to life plus a fine for the section 17 FT offence, imprisonment up to life and a fine for the section 21 offence of holding terrorism proceeds, and imprisonment up to 14 years and/or a fine for the section 40 offence of financing terrorist organisations. The level of fines has not been set in the legislation and is at the discretion of the court, so here the amount can be tailored to the financial capacity of the company. Overall, these penalties can be considered quite effective, proportionate and dissuasive. There is however an illogical discrepancy between the level of punishment for financing terrorist acts and persons, which would include terrorist groups (s.17), and the sanctions for financing terrorist organisations (s.40).

196. As with money laundering, legal persons are subject to parallel criminal, civil or administrative proceedings (see Section 2.1 of this report).

Recommendation 32 - Statistics

197. The Ministry of Home Affairs (MHA) administers the UAPA and maintains the statistics on FT offences in consultation with the law enforcement agencies (LEAs) and State Governments. Since the financial year 2006-2007, 105 cases of FT have been registered involving 231 suspects. 29 trials are pending starting from 2006, and one conviction was obtained in 2009. Assets with a value of INR 47 009 800 (approximately USD 850 000) have been seized/attached, with INR 411 000 (around USD 108 000) forfeited.

Statistics: Terrorist Financing Cases

| Descriptions | 2006-2007 | 2007-2008 | 2008-2009 | 2009-2010 (up to 31.12.2009) | Total |
|--|-------------------------------------|--|--|------------------------------------|------------|
| No. of FR cases registered | 17 | 25 | 36 | 27 | 105 |
| No. of persons accused for FT | 54 | 65 | 61 | 51 | 231 |
| Value of seizure/Attachment of assets (in INR) | 9 690 000 | 13 640 000 | 7 173 000 | 16 506 8000 | 47 009 800 |
| No. of charge sheet filed | 13 | 7 | 12 | - | 32 |
| Whether a provision of the UAPA was invoked. | Yes | Yes | Yes | Yes | - |
| Status of the trials | 12 trials in progress, 1 convicted. | 6 pending trials, 1 trial to commence. | 11 pending trials, 1 trial to commence | - | - |
| No. of challans ¹⁸ filed | - | 6 | 2 | - | 8 |
| No. of persons convicted | - | - | - | 1 ¹⁹ | 1 |
| Value of property forfeited (in INR) | 4 900 000 | 289 000 | 222 000 | - | 5 411 000 |
| No. of cases under investigation | 4 | 12 | 22 | 28 | 66 |

¹⁸ "Challan": charge sheet to be filed before Magistrate/Court of Sessions in a criminal case.

¹⁹ The case itself relates to the financial year 2006-2007.

Statistics: Other terrorist related figures

| SI No | ITEM | 2006 | 2007 | 2008 | 2009 | 2010 | Total |
|-------|---|-------|-------|-------|-------|-------|---------|
| 1 | INCIDENTS | 4 551 | 4 053 | 3 859 | 5 051 | 947 | 18 461 |
| 2 | CIVILIANS KILLED | 1 480 | 1 269 | 1 360 | 928 | 253 | 5 290 |
| 3 | SECURITY PERSONNEL KILLED | 415 | 440 | 387 | 446 | 68 | 1 756 |
| 4 | TERRORISTS KILLED | 1 265 | 1 133 | 1 188 | 1 027 | 217 | 4 830 |
| 5 | WEAPONS SEIZED | | | | | | |
| (i) | ASSAULT RIFLES | 794 | 756 | 522 | 415 | 106 | 2 593 |
| | <i>(Seized value in million INR)</i> | 47.64 | 45.36 | 31.32 | 24.90 | 6.30 | 155.52 |
| | <i>(Forfeited value in million INR)</i> | 34.30 | 31.30 | 25.68 | 19.17 | 4.79 | 115.24 |
| (ii) | SMALL ARMS | 758 | 720 | 1588 | 1 018 | 78 | 4 162 |
| | <i>(Seized value in million INR)</i> | 39.70 | 36.00 | 79.40 | 50.90 | 3.90 | 209.90 |
| | <i>(Forfeited value in million INR)</i> | 14.29 | 13.32 | 34.94 | 20.87 | 1.56 | 84.98 |
| (iii) | ROCKET LAUNCHERS | 31 | 5 | 20 | 11 | 3 | 70 |
| | <i>(Seized value in million INR)</i> | 3.10 | 0.50 | 2.00 | 1.10 | 0.30 | 7 |
| | <i>(Forfeited value in million INR)</i> | 2.70 | 0.35 | 1.46 | 0.99 | 0.25 | 5.746 |
| (iv) | GRENADES | 2 491 | 1 856 | 1 555 | 1 435 | 346 | 7 683 |
| | <i>(Seized value in million INR)</i> | 12.50 | 9.30 | 7.80 | 7.20 | 1.70 | 38.5 |
| | <i>(Forfeited value in million INR)</i> | 2.88 | 2.33 | 1.48 | 1.44 | 0.43 | 8.547 |
| (v) | EXPLOSIVES (kilograms) | 1 879 | 990 | 575 | 733.5 | 576 | 4 753.5 |
| | <i>(Seized value in million INR)</i> | 9.4 | 5 | 3 | 3.7 | 2.9 | 24 |
| | <i>(Forfeited value in million INR)</i> | 3.102 | 1.4 | 0.9 | 1.073 | 1.015 | 7.49 |

Statistics: Other seizures under the UAPA²⁰

| SI no | Item | 2006 | 2007 | 2008 | 2009 | 2010 | Total | Value (in million INR) |
|----------------------------|---|------|------|------|------|------|-------|---------------------------|
| Moveable Property | | | | | | | | |
| 1 | Vehicles (Car, truck, SUV, Motor cycle) | 3 | 4 | 7 | 3 | 3 | 20 | 11.92 |
| 2 | Boat | | 2 | 2 | - | - | 4 | 7.00 |
| Immoveable Property | | | | | | | | |
| 3 | Building | | 1 | | | | 1 | 3.00 |
| 4 | Commercial Establishments | | | 2 | | | 2 | 10.60 |
| | TOTAL | | | | | | | 32.52 |

²⁰ These statistics do not differentiate between the various asset categories (financing, instrumentalities, proceeds, or assets belonging to terrorist individuals/groups).

198. Two Special Courts have been established for the trial of terrorism related cases. At the time of the on-site visit, the NIA had been assigned three cases for investigation and prosecution, two of which relate to terrorist financing and one relates to counterfeit currency. The latter can be explained based on the finding that the financing of most terrorist acts of which India has been a victim is derived from internationally designated organisations and/or entities operating from safe haven countries, and using counterfeit currency notes.

Implementation and effectiveness

199. With the combined application of section 15 and section 17/section 40 of the UAPA India has taken steps to meet the international standards governing the criminalisation of terrorist financing. The Art. 2 requirement of the FT Convention is covered by the criminalisation of the financing of terrorist acts, as defined and listed in section 15 of the UAPA. This provision is meant to capture all activities falling within the scope of the FT Convention annexed Treaties (Art. 2.1(a)) and of the generic offence of Art. 2.1(b) of the FT Convention). It does not adopt the specific terminology used in the Treaties and the Convention to define the acts that according to the Convention are to be considered offences of a terrorist nature, but mostly translates these activities in more wide scope qualifications intended to cover all relevant terrorist acts in one provision. Thus, section 15 of the UAPA, contains a mixture of diverse clauses from the FT Convention without actually following its specific structure, which is perfectly acceptable as long as the principles and substance of the FT Convention are fully observed.

200. The UAPA approach however gives rise to following remarks and indications of (largely technical) deficiencies:

- a. Under Art. 2.1(a) of the FT Convention the sole act of financing the offences falling under the scope of or as defined in the annex Treaties should be criminalised as terrorist financing per se, without any further conditions or circumstances. Any (corresponding) act under section 15 however requires the additional and specific intent to “threaten the unity, integrity, security or sovereignty of India or intent to strike terror or likely to strike terror in the people or any section of the people in India or in any foreign country” before they qualify as terrorist acts.
- b. The Treaties offences derive their “terrorist” character from their very specific gravity, nature, object or target as such. The acts listed in section 15(a) largely refer to common criminal activity that only obtains its terrorist status when carried out with a specific intent. Consequently, the general terminology (“... *by any other means of whatever nature* ...”) used in section 15(a) of the UAPA cannot be considered as corresponding with the Treaties offences.
- c. The offence defined in Art. 7(d) of the Convention on the Physical Protection of Nuclear Material 1979 finds its correspondent offence of making demands for radioactive instances, nuclear devices, etc. in section 16A of the UAPA. This last provision is however not listed in section 15 as a terrorist act, and consequently is not covered by the terrorism financing offence of section 17 of the UAPA. Even if arguably the section 16A offence would qualify as a terrorist act because of its specific terrorist intent, then again the offence of financing such activity should be punishable as such and not be conditional to the “intention of aiding, abetting or committing a terrorist act”.
- d. Unlike section 15(c) of the UAPA, which is restricted to threats to governments and persons, the terrorist activity defined in Art. 2.1(b) of the FT Convention also includes an international organisation as a possible target. The definition of “person” in section 3 GCA (“*any company*”

- or association or body of individuals”)²¹ cannot reasonably be seen as covering such organisation, as was argued by the Indian authorities.
- e. The international standards call for the criminalisation of the wilful financing of terrorist individuals and terrorist organisations as such, without requiring the specific intention or knowledge that the funds could or should be used to commit a terrorist act (s.17 of the UAPA) or furthering the activity of a terrorist organisation (s.40 of UAPA)²².
 - f. The ancillary “attempt” offence is not satisfactorily covered in the UAPA. Section 17 does not cover the attempt to commit the financing offence of raising or collecting funds, while section 40 does not provide for the attempt at all. It was argued that the attempt (and other ancillary offences) is covered by section 18 of the UAPA, whereby the financing is seen as an “act preparatory to the commission of a terrorist act”. This may indeed be partially the case whenever such act is committed or prepared but, as indicated above, the FT offence does not necessarily have to be linked to any (prepared) terrorist act, as is the case when the funds are intended or used for non-terrorism purposes by a terrorist individual or organisation.
 - g. Although objectively the punishment for violation of the section 40 UAPA financing of a terrorist organisation offence (up to 14 years imprisonment and/or a fine) seems effective and dissuasive enough, it is disproportionately low compared with the sanctions provided for the offence of financing terrorist acts by section 17 of the UAPA, or for other terrorist related offences for that matter, which range from 5 years to life imprisonment and a fine. There are no objective grounds for discriminating between those offences that are quite similar in nature and gravity. One can even question the sense of maintaining section 40 of the UAPA anyway, as it seems outdated and made redundant by section 17 of the UAPA that includes the financing of terrorist groups (see above). By itself, however, the section 40 penalty level meets the cr. II.4/2.5 standard.
 - h. As for the circumstance of the corporate criminal liability application depending on the concurrent prosecution of a natural person, reference is made to the comments under the ML criteria (see Section 2.1. above).

201. The statistics show a fairly frequent application of the relevant criminalisation provisions by the prosecution. Since 2006, 29 FT prosecutions have been initiated on the basis of the UAPA, although the trial is still underway in 28 cases and only 1 case had ended up in a conviction at the time of the on-site visit²³. According to the authorities, this was not due to evidentiary challenges but to the fact that in view of the possible severe penalties the defence exhausts all legal procedural means of appeal in every step of the way, which because of the workload of the courts results in very lengthy proceedings. The very length of the court proceedings must be a matter of concern for the authorities, as this does create an impression of ineffectiveness.

202. The serious commitment of India - a country that is constantly confronted with the reality of terrorist activity - in combating terrorism in all its forms, as demonstrated by the figures above, must be acknowledged. Also, India is party to all Treaties annexed to the FT Convention and even goes beyond Art. 3 of the Convention that excludes its application to domestic terrorism²⁴.

²¹ Section 2(a) of the UAPA defines “association” as “any combination or body of individuals”.

²² See FATF Interpretative Note to SR II, “Characteristics of the Terrorist Financing Offence”, *par.* 3.

²³ Another 2 terrorist convicts were sentenced by a Delhi court to life imprisonment on 10 March 2010, *i.e.* on the basis of section 17 of the UAPA. It is not known if this conviction is final.

²⁴ It is estimated that ca. 70% of the terrorist activity in India falls in that category.

203. As for terrorist financing, from a law enforcement perspective this commitment is translated in an active pursuit of the financial aspects of terrorism, as witnessed by the sizable number of cases brought before the court that are at various stages of trial. They mark an appropriate focus and effort at prosecutorial level, which however is at present not convincingly followed up by convictions and firm case law. Furthermore, although the section 15 and section 17 UAPA provisions follow a certain logic that roughly reflects the international approach, they deviate from the standards on several aspects.

2.2.2 Recommendations and Comments

204. Although the fight against terrorism financing is actively pursued in India, as witnessed by the number of investigations and prosecutions, there are a number of deficiencies that need to be addressed to bring the offence more in line with the relevant international standards and, by doing so, enhance the effectiveness of the CFT system itself.

- The sole (intentional or knowing) financing of the offences covered by the Treaties annexed to the FT Convention should be criminalised as terrorist financing
- The section 16A UAPA offence of making demands for nuclear material, etc. should be included in the section 15 list of terrorist acts.
- The terrorist acts under section 15 of the UAPA should also target international organisations.
- The attempt to commit the section 17 and section 40 UAPA offences should be fully covered.
- The sole wilful financing of terrorist individuals and terrorist organisations should be criminalised.

2.2.3 Compliance with Special Recommendation II

| | Rating | Summary of factors relevant to s.2.2 underlying overall rating |
|-------|--------|---|
| SR.II | PC | <ul style="list-style-type: none"> • FT provisions not in line with the FT Convention: <ul style="list-style-type: none"> ○ criminalisation of Treaty offences not consistent with art. 2.1(a); ○ not all Treaty offences included in the list of terrorist acts; ○ international organisations not covered; ○ FT attempt is not fully covered. • No criminalisation of sole knowing funding of terrorist individuals and terrorist organisations. • Effectiveness issue: <ul style="list-style-type: none"> ○ minimal number of convictions. |

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis

Recommendation 3

Property subject to confiscation

Prevention of Money Laundering Act (PMLA)

Proceeds of crime

205. The Adjudicating Authority (a quasi judicial authority) can make an order under section 8(6) of the PMLA for the confiscation of property that is proceeds of crime and that has been previously attached

or seized. The PMLA defines proceeds of crime as “any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled (predicate) offence or the value of any such property” (s.2(1)(u)). Property is defined as “any property or assets of every description, whether corporeal or incorporeal, moveable or immovable, tangible or intangible and includes deeds and instruments evidencing title to, or interest in, such property or assets, wherever located” (s.2(1)(v)).

206. An investigation into a ML case begins with the registration of an Enforcement Case Information Report (ECIR). Property identified as being involved in money laundering is either seized by exercising the powers under sections 17 or 18 of the PMLA or is provisionally attached (*immobilia*) under section 5 of the Act. Section 17 provides for search of buildings, places, conveyances etc., and section 18 provides for search of persons under certain circumstances. These sections also provide for seizure of any property found as a result of such search. The property can then be detained for purposes of confiscation. Thereafter, under section 8 of the PMLA, a complaint can be filed within 30 days before the Adjudicating Authority requesting that such provisional attachment or seizure be confirmed, *i.e.* to state that the provisionally attached or seized properties are involved in money laundering.

207. Simultaneously, a complaint is filed before the Special Court constituted under section 45 of the PMLA to prosecute the ML offender(s). The prosecution proceedings relating to the scheduled offence are also transferred to this court. Upon conviction of the accused in the proceedings related to the scheduled offence and such order becoming final, the seized/provisionally attached property is confiscated by the Adjudicating Authority according to section 8(6) of the Act. The onus will be on the accused to prove that the property is not proceeds of crime (s.8(1) and 24). Conversely, property that has been attached without a direct link to a specific predicate offence or a charge being filed for such an offence cannot be confiscated in the absence of a conviction for a predicate offence. Sections 8(3)(a) and (b) provides that, in relation to any attached/seized property involved in money laundering, such attachment or retention of the seized property shall continue during the proceedings relating to any scheduled offence before a court and become final after the guilt of the person is proved in the trial court and the order of such trial court becomes final.

Intended instrumentalities

208. There is no definition of intended instrumentalities in the PMLA nor does the Act contain any specific provision covering these specific items. However, by virtue of section 65 of the PMLA, which states that the provisions of the CrPC shall apply, in so far as they are not inconsistent with the provisions of the PMLA regarding arrest, search and seizure, attachment, confiscation, investigation, prosecution and all other proceedings under the PMLA, intended instrumentalities can be seized and confiscated under sections 102 and 452 of the CrCP.

Narcotic Drugs and Psychotropic Substances Act (NDPS Act)

Proceeds of crime

209. Chapter V(A) of the NDPS Act provides for confiscation of property derived from or used in illicit traffic in narcotic drugs. The provisions apply *inter alia* to persons in respect of whom an order of detention has been made under the Prevention of the Illicit Traffic in Narcotics and Psychotropic Substances Act, 1988; persons who have been arrested or against whom a warrant or authorisation of arrest has been issued for the commission of an offence punishable under the NDPS Act with imprisonment for a term of ten years or more; and relatives and associates of such persons. When the competent authority confirms the finding that any property of such person is illegally acquired property, then confiscation of such property ensues.

210. Property can be confiscated from persons charged with a drug offence, their relatives or associates, or anyone who holds the property that was previously held by someone charged, unless they acquired it in good faith for adequate consideration (s.68A(2)).

Intended instrumentalities

211. Any goods used for concealing any narcotic drug or psychotropic substance which is liable to confiscation under the NDPS Act shall also be liable to confiscation (s.61). Based on this provision, instrumentalities intended for use in the commission of a drugs offence can also be confiscated.

Unlawful Activities (Prevention) Act (UAPA)

Proceeds of crime

212. Chapter V of the UAPA allows for confiscation of property that is proceeds of terrorism. Proceeds of terrorism is defined as “*all kinds of properties which have been derived or obtained from commission of any terrorist act or have been acquired through funds traceable to a terrorist act, irrespective of the person in whose name such proceeds are standing or in whose possession they are found, and includes any property which is being used, or is intended to be used, for the purpose of a terrorist organisation or terrorist gang*” (s.2 (g)). Property means “*property and assets of every description, whether corporeal or incorporeal, moveable or immovable, tangible or intangible and legal documents, deeds and instruments in any form including electronic or digital evidencing title to, or interest in, such property or assets, by means of bank credits, travellers’ cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit, cash and bank account including fund, however acquired*” (s.2 (h)).

213. Section 24(2) of the UAPA states that proceeds of terrorism, whether held by a terrorist or terrorist organisation or terrorist gang or by any other person and whether or not prosecuted or convicted, can be confiscated. Section 33(1) further provides for attachment of property of a person accused of an offence under Chapter IV (terrorist activities) or Chapter VI (terrorist organisation) of the UAPA. It is for the court to issue an order that all or any of the properties, moveable or immovable or both, belonging to that person, shall, during the period of such trial, be attached. Where a person has been convicted of such offence, the court may, in addition to any punishment, by order in writing, declare that any property, moveable or immovable or both, belonging to the accused and specified in the order, shall stand forfeited (s.33 (2)).

Intended instrumentalities

214. The definition of proceeds of terrorism includes instrumentalities intended to be used for the purpose of a terrorist organisation or a terrorist gang.

Code of Criminal Procedure (CrPC)

Proceeds of crime

215. Chapter VIIA of the CrPC (ss.105A to 105J) provides for identification, attachment or seizure or confiscation of property derived or obtained directly or indirectly, by any person as a result of criminal activity, including crime involving currency transfer or the value of any such property. According to section 65 of the PMLA, the provisions of the CrPC shall apply, in so far as they are not inconsistent with the PMLA.

Intended instrumentalities

216. Section 102 of the CrPC provides for seizure of any property which may be found under circumstances which create suspicion of the commission of any crime. Section 451 of the CrPC provides for custody and disposal of property pending trial. The property referred therein includes “*any property regarding which an offence appears to have been committed or which appears to have been used for the commission of any offence*”. Once the trial is concluded, the court may order for confiscation of the property under section 452 of the CrPC. These provisions are broad enough to cover instrumentalities intended for use in the commission of an offence.

Provisional measures

217. All four Acts (PMLA, NDPS Act, UAPA and CrPC) allow for the initial attachment or seizing of property to prevent dealing with property subject to confiscation. Property can be frozen or seized without prior notice under all four Acts.

218. The PMLA initially allowed for attachment of property under section 5 only when a person had been charged with a predicate offence. Through the amendments to the PMLA in 2009 (s.5(1)), the competent authority may now provisionally attach for a period not exceeding 150 days proceeds of crime in the possession of any person charged for having committed a scheduled offence and when they are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to confiscation. In addition, any property of any person may be attached if there is reason to believe that its non-attachment is likely to frustrate any proceedings. Consequently, these recent amendments to the PMLA allow proceeds of crime to be provisionally attached, seized and subsequently confiscated regardless of whose possession they are in. As indicated above, premises can be searched and property can be seized where there is reason to believe that a person has committed the money laundering offence or is in possession of proceeds of crime related to money laundering. Persons can also be searched and property seized if there is reason to believe that any person is in the possession of proceeds of crime. This is only possible if a predicate offence has already been registered with a magistrate under sections 157 and 173 of the CrPC, but the person does not yet have to be charged with money laundering at that point in time.

219. Section 68F of the NDPS Act allows for the freezing or seizing of property to prevent any dealings. Authorities can seize all property of the accused that is believed to be illegally acquired and the onus is then on the accused to prove that the property is not the proceeds of crime (s.68J).

220. Section 25 of the UAPA allows investigating officers to seize and attach property to prevent the property from being transferred or dealt with. Section 25(5) allows an investigating officer to seize any cash which is intended to be used for the purposes of terrorism, or forms part of the resources of a ‘terrorist organisation’. Moreover, cash found during a search which is intended to be used for terrorism can be seized. In addition, the definition of cash also includes assets such as credit or debit cards or cards that serve a similar purpose.

221. Section 102 of the CrPC provides for seizure of any property which may be alleged or suspected to have been stolen, or which may be found under circumstances which create suspicion of the commission of any offence.

Powers to trace property and protection of rights

222. Law enforcement agencies have broad powers to trace and identify property through sections 16 to 18 of the PMLA. In addition, section 68E of the NDPS Act gives broad powers to officers to trace and

identify property that could be proceeds of crime, including making inquiries, conducting investigations and surveys of any person, place, property or financial institution, etc.

223. The UAPA (s.43(F)) confers powers to the officer investigating any offence under the UAPA to require any officer or authority of the Central Government or a State Government or a local authority or a bank, or a company, or a firm or any other institution, establishment, organisation or any individual to furnish information in his or its possession in relation to such offence, on points or matters, where the investigating officer has reason to believe that such information will be useful for, or relevant to, the purposes of the Act. Failure to furnish the information requested or deliberately furnishing false information is punishable with imprisonment for a term of up to three years or with a fine or with both.

224. Furthermore, sections 93 and 102 of the CrPC also confer powers on the investigating authorities to conduct searches of premises and persons and to seize assets.

Third party rights

225. The PMLA, NDPS Act and UAPA provide protection for the rights of bona fide third parties. Under the PMLA third parties that have an interest in the property attached have an opportunity to prove that the property is not involved in money laundering (ss.8, 17, and 18). In addition, persons who have a right to enjoy immovable property can still do so after the property is attached (ss.5 and 8). Under the NDPS Act property can be confiscated from a person charged with a drug offence or their relative, associate or holder of property that was previously held by someone charged. Holders that are transferees in good faith for adequate consideration are protected under sections 68A(2)(f) and 68B(g)(A). The UAPA also provides for protection of third parties and a possibility to appeal (s.25(6)). No confiscation shall be made if a person establishes that he is a bona fide third transferee of proceeds of terrorism without knowing that they represent such proceeds (s.27(2)). Section 30 of the UAPA also provides for claims by a third party.

Voiding of actions

226. Section 9 of the PMLA vests upon the Adjudicating Authority the power to declare void any encumbrances or lease-hold interests which have been created in the property attached under section 5 or seized under sections 17 or 18 with a view to defeat the provisions of the Act. The NDPS Act (s.68(M)) and the UAPA (s.32) allow for steps to be taken to void actions where property is transferred after a notice for attachment or confiscation is issued.

Additional elements

227. The UAPA allows the property of organisations listed as terrorist organisations in the Schedule to the UAPA and terrorist gangs to be frozen under section 7 and confiscated through the usual confiscation provisions. In addition, State Acts such as the Uttar Pradesh Gangster and Anti-Social Activities (Prevention) Act, 1986 (s.14) and the Maharashtra Control of Organised Crime Act, 1999 (s.20) deal with the confiscation of property of criminal organisations.

228. Confiscation without conviction (civil forfeiture) is not currently available in the PMLA. Chapter V(A) of the NDPS Act provides for civil forfeiture of property derived from or used in illicit traffic in narcotic drugs. Section 24(2) of the UAPA allows for the proceeds of terrorism to be confiscated without a conviction.

229. As indicated above, the onus will be on the accused to prove that assets are not the proceeds of crime (PMLA s.24). In addition, section 8(1) of the PMLA stipulates that the Adjudicating Authority may call upon any person that has committed the ML offence to indicate the sources of his income, earning or assets out of which or by means of which he has acquired the property attached or seized. The burden of

proof is also on the offender in the NDPS Act (s.68J); the UAPA (s.27(2)); the CrPC (s.105 G) and the Maharashtra Control of Organised Crime Act (s.4).

230. Trial in absentia of the defendant is not recognised in the Indian legal system. If the accused is not given full opportunity of being heard, it is considered a violation of the principle of natural justice. However, under section 82 of the CrPC, a defendant who has absconded or is concealing himself can be declared a proclaimed offender and, under section 83 of the CrPC, the trial court can order attachment of any property of the proclaimed offender. Under section 85 of the CrCP the attached property shall be at the disposal of the State Government if the proclaimed person does not appear within the time specified in the proclamation.

Recommendation 32 - Statistics

231. Statistics regarding the confiscation under the PMLA are maintained by the Directorate of Enforcement while statistics regarding the confiscation of illegally acquired property under the provisions of the NDPS Act are maintained in the Department of Revenue. The statistics regarding underlying predicate offences are maintained by the National Crime Record Bureau (NCRB) which publishes crime statistics on its website (<http://ncrb.nic.in>). The statistics pertaining to seizure/confiscation of the proceeds of crime by State LEAs under the provision of the CrPC and special laws are not maintained by the Central Government or any federal agency.

Statistics: Money Laundering cases (value in INR)

| | Items | 2006-2007 | 2007-2008 | 2008-2009 | 2009-2010 (31 December 2009) | Total |
|----|--|------------|-------------|-------------|---------------------------------|---------------|
| 1. | No. of ECIRs | 27 | 15 | 17 | 739 | 798 |
| 2. | No. of Provisional orders passed for attachment | 7 | 05 | 22 | 9 | 43 |
| 3. | Value of provisionally attached property | 10 200 000 | 330 500 000 | 424 400 000 | 2 242 500 000 | 3 007 600 000 |
| 4. | No. of Provisional attachments orders confirmed by AA | 3 | 8 | 16 | 13 | 40 |
| 5. | Value of provisionally tainted assets confirmed by AA | 4 800 000 | 48 400 000 | 583 700 000 | 109 600 000 | 746 500 000 |
| 6. | No. of Provisional attachment orders (PAOs) under confirmation/pending before the AA | - | - | 1 | 3 | 4 |
| 7. | No. of PAOs not confirmed by the AA | - | - | 1 | - | 1* |
| 8. | Value of assets in respect of PAOs not confirmed by the AA | - | - | 38 000 000 | - | 38 000 000 |
| 9. | No. of appeals filed before Tribunal | | | | | |
| | By the Party | - | 3 | 15 | 14 | 32 |
| | By the Directorate | - | - | 1 | - | 1 |

* Appeal filed by the Department before the Tribunal.

232. In addition, instrumentalities amounting to INR 13 million have been seized/attached under the PMLA. These instrumentalities include motor vehicles, equipments, etc.

Implementation and effectiveness

Prevention of Money Laundering Act (PMLA)

233. Confiscation under Chapter III of the PMLA is only possible when it relates to “proceeds of crime” as defined in s. 2(1)(u), *i.e.* resulting from a scheduled offence, and when there is a conviction of such scheduled (predicate) offence. In addition, in such cases, only proceeds of the predicate offence can be confiscated and not the proceeds of the ML offence itself.

234. The predicate offence conviction condition creates fundamental difficulties when trying to confiscate the proceeds of crime in the absence of a conviction of a predicate offence, particularly in a stand-alone ML case, where the laundered assets become the *corpus delicti* and should be forfeitable as such. In the international context, the predicate conviction requirement also seriously affects the capacity to recover criminal assets where the predicate offence has occurred outside India and the proceeds are subsequently laundered in India (see also comments in Section 2.1 above).

235. The definitions of proceeds of crime and property in the PMLA are broad enough to allow for confiscation of property derived directly or indirectly from proceeds of crime relating to a scheduled (predicate) offence, including income, profits and other benefits from the proceeds of crime. These definitions also allow for value confiscation, regardless of whether the property is held or owned by a criminal or a third party. As section 65 of the PMLA refers to the rules in the CrPC, instrumentalities and intended instrumentalities can be confiscated in accordance with sections 102 and 451 of the CrPC. However, there is no case law in this respect.

236. Also, the procedural provisions of Chapter III make confiscation of the proceeds of crime contingent on a prior seizure or attachment of the property by the Adjudicating Authority, and consequently substantially limit the possibilities for confiscation under the PMLA.

237. There have been no convictions for money laundering under the PMLA and no property has been confiscated under this Act. Since 2006, the Adjudicating Authority has, however, confirmed 40 orders of provisional attachments.

Narcotic Drugs and Psychotropic Substances Act (NDPS Act)

238. The confiscation regime under the NDPS Act is quite narrow. It is possible to confiscate proceeds of drug offences under the NDPS Act, but only where a warrant for the arrest of a person has been issued for an offence punishable with imprisonment for more than 10 years or a similar offence in another country. This applies both to the proceeds of drug offences and the drug related money laundering. Instrumentalities can be confiscated if they are goods used for concealing narcotic drugs (section 61). Property of corresponding value cannot be confiscated under the NDPS Act. So, the NDPS Act only allows for confiscation in very limited circumstances, where there are proceeds or particular instrumentalities of some specific drug offences.

239. There has not been any court case where proceeds of crime or instrumentalities have been confiscated as a result of a conviction for drug related money laundering. There have been a number of confiscation actions under the NDPS Act but none related to money laundering.

Unlawful Activities (Prevention) Act (UAPA)

240. Confiscation of property that is proceeds of terrorism, held by terrorists or terrorist groups, is provided for in section 24(2) of the UAPA. There is however a discrepancy between this provision and the definition of ‘proceeds of terrorism’, which according to s.2(1)(g) includes property which has been derived or obtained from the commission of a terrorist act or has been acquired through funds traceable to a

terrorist act, including any property which is being used, or is intended to be used, for the purpose of a terrorist organisation or terrorist gang. Based on this definition, the UAPA allows for the confiscation of proceeds that are the results of a committed terrorist act and funds benefiting terrorist groups. As the definition does not cover the funding of individual terrorists or future terrorist acts, the UAPA does not allow for the confiscation of property in these particular circumstances. Confiscation of assets not (directly) related to a terrorist offence is however possible under section 33 of the UAPA, according to which a court can order the attachment of all assets belonging to a person accused of terrorist offences, and the forfeiture of these assets upon conviction.

241. Section 25(5) of the UAPA allows for seizure of proceeds of terrorism in relation to an investigation of a terrorist activity or a terrorist organisation. The law also provides for seizure of cash which is intended to be used for the purpose of terrorism. The reference in section 2(g) of the definition of financing of terrorism to “*any property which is being used, or is intended to be used*” is broad enough to also include intended instrumentalities used in the FT context, although, as noted above, limited to terrorist groups only.

242. The UAPA does not provide for the confiscation of property of corresponding value as such. However, to a certain extent, section 33 of the UAPA goes in that direction in providing for the attachment and subsequent confiscation of assets unrelated to the offence and can be used to achieve a somewhat similar effect, without however fully corresponding with the concept of a comprehensive equivalent value confiscation. This measure is not linked with instances where assets subject to confiscation should have disappeared or are unavailable nor is the amount linked to that of the dissipated assets.

243. Three non-conviction forfeiture procedures have been conducted under the UAPA (ss.25 and 26) and there has been one case of criminal procedure confiscation (see Section 2.2. above).

General comments

244. Since confiscation is linked to a conviction it is not possible to confiscate criminal proceeds when the defendant has died during the criminal proceedings. However, it is possible to attach and dispose of any property of a proclaimed offender when that person has absconded. The absence of a regulation when the defendant has died may have a negative impact on the effectiveness of the confiscation regime in place in India.

245. The effectiveness of the confiscation provisions under the PMLA, the NDPS Act, and the UAPA, cannot be assessed due to the low numbers of confiscations under these Acts. However, confiscations of proceeds derived from predicate offences are frequent under the IPC and other laws as shown in Annex 5.

2.3.2 Recommendations and Comments

246. Although the confiscation regime in India allows for a broad spectrum of seizure and forfeiture measures in the AML/CFT context, it is not fully comprehensive and does show a number of (legal) deficiencies. Therefore it is recommended that:

- Legal measures are taken to allow for confiscation of the money laundered as subject of the ML offence and which is not contingent on a conviction for the predicate offence (stand-alone ML offence).
- The Indian authorities ensure that the definition of proceeds of terrorism is wide enough to allow for confiscation of instrumentalities and funds used to finance an individual terrorist and terrorist acts.
- The UAPA and the NDPS Act should explicitly provide for full equivalent value confiscation.

- The confiscation regime should also include clear provisions and procedures on how to deal with the assets in case the criminal proceedings come to a halt because of the death of the suspect.
- India should consider consolidating all seizing and confiscation provisions into one Act, especially with regard to money laundering, to provide a simpler system and a consistent treatment for all proceeds of crime.

2.3.3 Compliance with Recommendations 3

| | Rating | Summary of factors relative to s.2.3 underlying overall rating |
|-----|--------|--|
| R.3 | PC | <ul style="list-style-type: none"> • Confiscation of property laundered is not covered in the relevant legislation and depends on a conviction for a scheduled predicate offence. • The UAPA does not allow for confiscation of intended instrumentalities used in terrorist acts or funds collected to be used by terrorist individuals. • The UAPA and NDPS Act do not allow for property of corresponding value to be confiscated. • There are no clear provisions and procedures on how to deal with the assets in case of criminal proceedings when the suspect died. • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns based on the limited number of confiscations in relation to ML/FT offences. |

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

Special Recommendation III

Laws and procedures to freeze pursuant to S/RES/1267(1999)

247. India has issued the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007 (the 2007 Order), pursuant to the United Nations (Security Council) Act, 1947. The provisions in the 2007 Order enable the Indian Government to freeze assets pursuant to UNSCRs 1267, its successor resolutions and 1373. In view of giving effect to the updated Security Council list, the 2007 Order is amended from time to time, with the last amendment made in July 2009. The 2007 Order provides the Central Government with broad powers to prevent and suppress terrorist acts falling within the Security Council Resolutions. It also contains a Schedule, which lists all the persons to whom the 2007 Order applies. The 2007 Order sets out general principles and powers. It allows the Government to issue all directions to authorities it may consider necessary for the implementation of the 2007 Order.

248. Terrorist organisations can also be listed under a separate process in the schedule to the UAPA, which allows for the freezing, seizing and attachment of their assets. The 2008 amendment to the UAPA includes a provision in the Schedule attached to the UAPA which allows that all the persons/entities designated by the UN Security Council and which have been notified by India under the 2007 Order, will *ipso jure* be considered a terrorist organisation in India to which the provisions of the UAPA apply. The UNSCR 1267 list is therefore automatically incorporated into the Schedule to the UAPA as soon as the Ministries are notified of the new names. The initial freezing is an administrative process and does not need a court order, as the necessary Gazette notification has already been issued through the UN Security Council Act. However, if assets are to be forfeited, a court order is required under the forfeiture provisions of the UAPA. A detailed procedure for seizures, attachment and forfeiture of proceeds of terrorism is provided under chapter V of the UAPA (see also section 2.3 above).

249. In addition, the 2008 amendment to the UAPA has also inserted another specific provision in section 51A by virtue of which the Central Government has direct powers to give effect to S/RES/1267(1999) and S/RES/1373(2001) and the administrative freezing procedures. The Internal Security-I Division of the Ministry of Home Affairs (IS-I of the MHA) has issued instructions and guidance (Order F. No. 17015/10/2002-IS-VI) on 27 August 2009 outlining the procedure for the implementation of this new provision in the UAPA to ensure that freezing would take place without delay and without prior notice to the designated individuals/entities. For the purposes of this report, these instructions and guidance issued in the form of an Order are further referred to as the MHA Guidance.

Laws and procedures to freeze pursuant to S/RES/1373(2001)

250. The procedures outlined above in relation to S/RES/1267(1999) equally apply to S/RES/1373(2001). India maintains a list of its own designated terrorist organisations based on section 35 of the UAPA and this list is published in the Schedule attached to the UAPA. It is also shared with other countries. The list currently contains 34 entities as designated terrorist entities, including those individuals/entities mentioned in the 2007 Order issued pursuant to UN Resolutions.

251. The pieces of legislation described above do not contain any specific provisions to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions. However, the Indian authorities state that this would be taken care of under section 51A in the UAPA which contains the words “or any other person engaged in or suspected to be engaged in terrorism”.

252. It should be noted, that the MHA Guidance issued pursuant to section 51A of the UAPA, contains the procedure to be followed with regard to foreign listing requests: the Ministry of External Affairs (MEA) shall examine requests made by foreign countries and forward them with its comments to the MHA. If the MHA, after examination, is satisfied that the person or entity concerned is a terrorist or a terrorist organisation, it shall forward the request to the financial sector regulators and the FIU-IND. Thereafter the normal procedure for freezing shall be followed.

Scope of “property” to be frozen

253. Chapter V of the UAPA deals with the procedure for seizure, attachment and forfeiture of proceeds of terrorism. Proceeds of terrorism are defined in section 2(1)(g) of the UAPA to include “*all kinds of properties which have been derived or obtained from commission of any terrorist act or have been acquired through funds traceable to a terrorist act, irrespective of the person in whose name such proceeds are standing or in whose possession they are found, and includes any property which is being used, or is intended to be used, for the purpose of a terrorist organisation or a terrorist gang*”. The punishment for holding proceeds of terrorism is dealt with under section 21 of the UAPA and is applicable to the entities listed in the Schedule but also to unlisted terrorist groups (see Section 2.2 above).

254. Based on Section 51A of the UAPA, the Central Government has the power to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the 2007 Order, or by any other person engaged in or suspected to be engaged in terrorism. The Central Government can also prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the 2007 Order or any other person engaged in or suspected to be engaged in terrorism. This provision implies that any funds or assets which are jointly held by a terrorist or terrorist organisation, either with a non-terrorist or a terrorist or a terrorist organisation are also covered.

Communication and guidance

255. Paragraph 2 of the MHA Guidance provides for the appointment of and the provision of details about officers designated under the UAPA responsible for receiving/providing the relevant information while paragraph 3 lists the authorities to which the list of designated individuals/entities needs to be communicated. Paragraph 4 of the MHA Guidance gives instructions on how the financial sector entities have to deal with funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. Based on paragraph 3, the MEA is responsible for updating the list of persons and entities subject to UN sanctions measures and providing it to the financial sector regulators (RBI, SEBI and IRDA), the FIU-IND and the MHA. It is the role of the regulators to forward the updated list to the banks, the stock exchanges, depositories, the intermediaries regulated by SEBI and the insurance companies. The MHA forwards the lists of designated individuals/entities to the UAPA officers in charge of all States and Union Territories and also provides these lists to the immigration authorities and security agencies.

256. Based on paragraph 4 of the MHA Guidance, the RBI, SEBI and IRDA are mandated to issue necessary guidelines to banks, stock exchanges, depositories, intermediaries regulated by SEBI and insurance companies concerning their obligation to take action regarding the freezing mechanism in place.

257. The MHA Guidance dated 27 August 2009 makes it very explicit that in case the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges, depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions. They need to notify without delay the Joint Secretary (IS-I) of the MHA, electronically and also over phone and fax. The effect of this instruction is that the freezing mechanism comes into play immediately, as all transactions are stopped. Hence, de-facto, the freezing by the banks, stock exchanges, depositories, intermediaries regulated by SEBI and insurance companies, ensures that the freezing takes place without delay. The entire purpose of the freezing action is to ensure that the designated individual/entity is denied access to the assets and this is ensured by the transaction being stopped. In such cases, the reference directly made by the institution concerned to the IS-I division of the MHA is followed up by the issuance of a formal order under section 51A, within 24 hours of the receipt of the notification by the financial institution.

258. In case of insufficient particulars (a single match, for instance: only a name), the reporting institutions have also the obligation to make a reference to the MHA's IS-I division, however, the procedure to be followed within this division will be different. On receipt of the particulars identified by the reporting institutions, the IS-I division may ask for a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the reporting entities are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by reporting institutions are held by the designated individuals/entities. This verification would be completed within a period not exceeding five working days from the date of receipt of such particulars. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA is to be issued within 24 hours of such verification and conveyed electronically to the concerned branch of the institution with a copy to the regulator and the FIU-IND.

259. The RBI Master Circular issued on 1 July 2009 for banks states that when new lists are issued in accordance with the UNSC Resolutions and are received from the Government of India, banks are advised that before opening a new account they should be convinced that the name of the customer does not appear in the list. Furthermore, banks should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing a resemblance with any of the individuals or entities in the list should immediately be reported to the RBI and the FIU-IND, in addition to the initial report to be made to the MHA.

260. In addition, the RBI has issued, on 17 September 2009, a Circular for Scheduled Commercial Banks and all financial institutions following the MHA Guidance issued at the end of August 2009. It is indicated that the RBI will forward upon receipt from the Government of India the names and other details of individuals/entities added to the lists. Such an updated version was issued by the RBI on 11 November 2009. Similarly, in its Master Circular issued on 24 November 2008, IRDA gives guidance in this regard to insurance companies. This guidance has been completed by IRDA's circular of 28 October 2009, following the MHA Guidance, outlining the new procedure to be followed based on section 51A of the UAPA.

261. SEBI has also issued guidance in this regard on 1 September 2009 where a reference is made to the UNSC lists. Registered intermediaries are directed that before opening any new account, they must be assured that the name(s) of the proposed customer does not appear on the UNSC lists. Further, registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in these lists. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to SEBI and FIU-IND²⁵.

Procedures for delisting, unfreezing and obtaining access to frozen funds

262. The Central Government has the powers to de-list any designated organisation pursuant to section 36 of the UAPA, which explains the procedure the Central Government will use for the exercise of its power under section 35(1)(c) to remove an organisation from the Schedule to the UAPA. As indicated above, the UNSC lists, as amended from time to time, are circulated by the MEA to the Regulators in view of taking appropriate actions in this regard. Such communications from the MEA also include the details of de-listed individuals and entities. Upon official de-listing of any individual or entity, the property and assets can be unfrozen and the asset holder can approach the appropriate authority to claim the assets/property.

263. The MHA Guidance contains the procedure for unfreezing of funds, financial assets, economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a terrorist or terrorist organisation. In addition, sections 25, 27, 28 and 30 of the UAPA also provide affected persons with an opportunity to seek appeal in a High Court for unfreezing blocked assets.

264. There are no legal provisions to access part of frozen funds for basic expenses. On 29 October 2009, the MEA has, however, instructed the RBI, SEBI, IRDA and FIU-IND that any request based on the provisions of UNSCR 1452 received by banks, stock exchanges, depositories, intermediaries regulated by SEBI and insurance companies needs to be forwarded to the MHA for further consideration. The person affected could also get free legal aid from the court. The expenses on account of medical treatment of an accused in Police custody or judicial custody are the expenses of the Government.

²⁵ On 22 February 2010 (this is ten days after the two months period following the on-site visit), India has also issued guidelines to sensitise the DNFBP sector. These guidelines focus on the provisions of section 51A of the UAPA and the general MHA Guidance issued on 27 August 2009. They were provided to the Institute of Chartered Accountants, the Institute of Cost and Works Accountants, the Institute of Company Secretaries of India, and the Registrar of Companies and highlighted the procedure to be followed by them and their members. On the same day, a similar communication was issued to the Principal Secretaries (Home) of all States and Union Territories in respect of dealers in precious metals and stones and the Registrars of Societies, firms and NPOs. Apart from the above, a separate communication (also dated 22 February 2010) containing similar provisions for casinos was sent to the Chief Secretary of Goa.

265. Under the Indian legal system any freezing order is subject to challenge before a court of law. The UAPA through its sections 25(6), 27 and 28 provides a procedure through which a person or entity whose funds or other assets have been frozen can challenge that measure in the court. Apart from the provisions in the UAPA, the person or entity concerned has also a right to a constitutional remedy and can approach the High Court on the basis of Articles 226 and 227 of the Constitution of India.

Freezing, seizing and confiscation in other circumstances

266. The normal procedures in the UAPA relating to seizure, attachment and forfeiture of proceeds of terrorism apply (for more details see Section 2.3 of this report).

Rights of third parties

267. A bona fide third person or entity whose funds or other assets have been frozen can file objection before the designated authority under section 25(3) of the UAPA and can also challenge that measure in a Court of law (ss.25(6) and 30 of the UAPA). In addition, the person or entity concerned has the right to avail constitutional remedy by approaching the High Court under Articles 226 and 227 of the Constitution of India.

Monitoring and sanctions

268. The MHA monitors the implementation of the prescribed procedures by the competent authorities. As indicated above, the financial sector regulators (RBI, SEBI and IRDA) are expected to have mechanisms in place to monitor compliance with the guidance, and to impose sanctions of administrative, civil and criminal nature to ensure compliance.

Recommendation 32 - Statistics

269. The MHA maintains statistics on offences of terrorist financing in consultation with the law enforcement agencies and State Governments. Property of a designated individual, valued at more than INR 1.5 billion has been seized, attached and forfeited by the Indian law enforcement authorities and courts based on the provisions of Indian Laws. Two bank accounts suspected to be involved in FT have been frozen under section 51 A of the UAPA. These two bank accounts fall under the application of UNSCR 1373 (domestic terrorist) and have been frozen on the basis of the freezing mechanism in place.

Implementation and effectiveness

270. There are provisions in the UAPA which allow for freezing of terrorist funds or other assets of persons and entities designated in accordance with S/RES/1267(1999) and S/RES/1373(2001). The MHA has also issued Guidance in this respect. Based on the MHA Guidance, the regulators (RBI, SEBI, and IRDA) have issued circulars with more detailed instructions and guidelines. The institutions supervised for AML/CFT purposes are also regularly updated of new designations of terrorist individuals or entities via amendments to the aforementioned circulars issued by their respective regulators. The MHA Guidance and regulators' circulars also cover the de-listing of terrorists and terrorist organisations and the procedures to follow for unfreezing funds.

271. India has an adequate system for freezing terrorist related assets. However, at the time of the on-site visit and until recently detailed instructions on how to deal with such assets were only available for the regulated financial institutions. The MHA has issued additional guidelines on 22 February 2010 (ten days after the two months following the on-site visit and outside the scope of this mutual evaluation) for the DNFBP sector, but to date, there is no indication that any of these instructions are effectively implemented. In addition, with the exception of the financial sector, there are no appropriate measures in place to monitor the compliance with the relevant legislation and guidelines and to impose sanctions for non-compliance.

272. India has mechanisms in place that enable it to freeze assets based on lists from other jurisdictions. In that regard, it should be noted that the circulars issued by the competent supervisory authorities for the financial sector include also the EU lists of terrorists and terrorist organisations.

273. When funds are frozen, the affected person has no access to assets necessary for basic expenses. Even though the MHA has informed the financial sector regulators that it will consider such requests made on the basis of the provisions of UNSCR 1452, there are no safeguards that the person will indeed have access to assets for basic expenses. The person can, however, get free legal aid. There are procedures in place through which a person or entity whose funds have been frozen can challenge that measure by having it reviewed by a court and the assessment team was informed about one case the Supreme Court dealt with in this respect. Furthermore, the rights of bona fide third parties are adequately covered.

274. All financial institutions the assessment team met with, but one, stated that they had never identified a perfect match with any of the terrorists or terrorist organisations on any of the lists. However, they had all identified partial names matches and had informed the MHA and the FIU-IND according to the procedures in place. The one institution that did identify a perfect match immediately blocked the account and filed an STR to the FIU-IND because at that time, the mechanism set out in section 51A of the UAPA was not yet in place. The other accounts were only blocked for a certain period of time (the time it took the MHA to determine if it was a perfect match or a false positive) but most of them were not frozen because the further analysis and investigation led to the conclusion that the possible match disclosed turned out to be a false positive.

2.4.2 *Recommendations and Comments*

275. Even though since 2007, India has introduced legislation and procedures that enable it to freeze terrorist funds, there still remain some shortcomings. It is therefore recommended that the Indian authorities ensure that:

- The guidelines recently issued for the DNFBP sector regarding the freezing mechanism are effectively implemented.
- A monitoring mechanism is set up to ensure compliance with the freezing mechanism outside the financial sector.
- Procedures are put in place for authorising access to funds for basic expenses.

2.4.3 Compliance with Special Recommendation III

| | Rating | Summary of factors relative to s.2.4 underlying overall rating |
|--------|--------|--|
| SR.III | LC | <ul style="list-style-type: none"> • There is no indication of effective implementation of the guidelines recently issued for the DNFBP sector. • There is no monitoring mechanism in place to ensure compliance with the freezing mechanism outside the financial sector. • There are no procedures in place that allow affected persons to have access to funds for basic expenses. |

Authorities

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and Analysis

Recommendation 26

Functions and responsibilities, operational independence and autonomy

276. Section 12 of the Prevention of Money Laundering Act (PMLA) requires every banking company, financial institution or intermediary to furnish information of all prescribed transactions to the Director in a timely manner as prescribed. The term “Director” is defined in section 2 of the PMLA, and means a Director, Additional Director, or Joint Director appointed under section 49 of the PMLA. Chapter VIII of the PMLA, entitled “Authorities”, provides for the appointment of specified Authorities for the purposes of the PMLA, and section 49 states that the Central Government may appoint such persons as it thinks fit for the purposes of being Authorities under the PMLA.

277. On 18 November 2004, the Government of India issued an Office Memorandum (OM – reference: No.4/10/2004-ES) to establish the Financial Intelligence Unit, India (FIU-IND), whose purpose is to co-ordinate and strengthen the collection and sharing of financial intelligence. The OM states that the FIU-IND is established as an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

278. The OM also establishes an officer of the rank of Joint Secretary to the Government of India to be the Director of the FIU-IND. As such, the Director is able to ensure operational independence and autonomy from undue influence or interference. Subsequently, on 1 July 2005, the Government of India published in the Gazette of India a Notification (reference: G.S.R.No.439(E)) granting exclusive and concurrent powers, contained in the PMLA, to the Director of the FIU-IND, including the power:

- a. to receive information on transactions from the reporting entities within the prescribed time (s.12(1)(b));
- b. to call for records referred to in section 12(1) and make such inquiry or cause such inquiry to be made, as he thinks fit (s.13(1));
- c. to levy a fine to the reporting entities for failure to comply with section 12 which shall not be less than INR 10 000 (USD 200) but may extend to INR 1 000 000 (USD 20 000) for each failure (s.13(2)); and
- d. of discovery and inspection, enforcing the attendance of any person, compelling the production of records, receiving evidence on affidavits, issuing commissions for the purposes of section 13 (s.50(1)).

279. The FIU-IND has been designated in the OM as the central national agency for receiving, processing, analysing and disseminating information relating to suspect financial transactions. The FIU-IND is also responsible for co-ordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering, terrorist financing and related crimes. The main functions of the FIU-IND as listed in Annex 2 of the OM can be summarised as follows:

- a. Collection of Information: act as the central reception point for receiving Cash Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) from various reporting entities;
- b. Analysis of Information: analyse received information to uncover patterns of transactions suggesting suspicion of money laundering, terrorist financing and related crimes;
- c. Disseminating/Sharing of Information: share information with national intelligence/law enforcement agencies, regulatory authorities and foreign Financial Intelligence Units (FIUs);
- d. Act as Central Repository: establish and maintain a national database on cash transactions and suspicious transactions on the basis of the reports received from reporting entities;
- e. Co-ordination: co-ordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering, terrorist financing and related crimes;
- f. Research and analysis: monitor and identify strategic key areas on ML trends, typologies and developments.

280. The FIU-IND adopts a hybrid distribution of work under which designated groups are assigned both sector and functional responsibilities which ensures exposure to the core functions of the FIU and also builds specialised skills. At present, six designated groups are formed within the FIU-IND, each led by an Additional Director with one or two Senior Technical Officers and support staff.

281. Each of the designated groups is allocated a set of reporting entities/sector (sector distribution), which assists to ensure involvement of senior management in the core functions of the FIU (*i.e.* analysis and dissemination). Sector responsibilities of each group include:

- a. conducting training;
- b. processing STRs;
- c. providing feedback to the allocated reporting entities or sectors; and
- d. allocated agency liaison (relationship, references, training).

282. In addition, the areas of work which are functionally distributed among the designated groups are:

- a. policy review;
- b. issues related to the FATF, the APG, and the Egmont Group;
- c. combating terrorist financing;
- d. ensuring compliance;
- e. exchange of information with foreign FIUs;
- f. negotiation of Memoranda of Understanding (MOUs) with foreign FIUs;
- g. analysis of CTRs;
- h. trend analysis of reports.

283. The FIU-IND Annual Report for 2007-2008 noted that it had just completed the FIUs second complete year of operation in the true sense - as such the FIU had, at the time of the on-site visit, been fully operational for just over three years.

Access to information (financial, administrative and law enforcement information)

284. The PMLA provides the FIU-IND with the statutory basis upon which to access financial, administrative and law enforcement information from various sources for analysis of STRs and processing of references received from other agencies (s.13 of the PMLA – see above).

285. Section 54 of the PMLA authorises and requires various agencies, such as the law enforcement authorities, the intelligence agencies, the tax authorities, the customs, the supervisory authorities, and reporting entities to assist the FIU-IND, when enforcing the provisions of the PMLA. Each agency has appointed a *nodal* officer to facilitate interaction with the FIU, and meetings to further streamline the exchange of information are organised on a regular basis.

286. In addition to transmitting requests through *nodal* officers, the FIU-IND has online access (through a batch file upload mechanism) to the Central Board of Direct Taxes' (CBDT) database of Permanent Account Numbers (PAN), issued by the tax authorities, the Corporate Database (MCA21) of the Ministry of Corporate Affairs (MCA), and the Foreign Contribution (Regulation) Act (FCRA) Database of the MHA. Since the Central Economic Intelligence Bureau (CEIB) has restructured the format of its database regarding Currency Declaration Forms (CDFs) (see description in Section 2.7 below), the FIU has integrated the CDF database in its analytical search engine. Access to additional information from all other government agencies, including tax information, is provided to the FIU upon request on a case-by-case basis. The FIU informed the assessment team that it receives effective responses to requests for information from other government agencies. In addition, the FIU indicated that the time taken on obtaining requested information depends on the complexity of the search required and the priority attached to it by the FIU. In case of priority requests, the *nodal* officers provide a response on the same day or within a couple of days.

287. The FIU-IND has powers under section 13(1) of the PMLA to obtain additional information from reporting entities. In addition, section 50 of the PMLA provides that for purposes of section 13, the Director of the FIU-IND shall have the same powers as a civil court in matters such as inspection, enforcing the attendance of any person, compelling the production of records, and receiving evidence on affidavits. Every financial institution can be requested to provide additional information, even if one particular entity has not disclosed an STR or CTR to the FIU. Based on its legal authority to obtain additional information, the FIU-IND states that in practice, it regularly receives such information from reporting entities for the analysis and processing of STRs and other references. This information relates to KYC details, including information collected during enhanced CDD, and account statements.

288. In practice, STRs received are processed and analysed by the designated analytical group. STR and CTR information is held on the FIU database, and STR information is matched with the information in this database and with other related information (such as relevant information received from the CEIB regarding CDFs) and, if necessary, further information is requested from the reporting entities, concerned regulators, intelligence and enforcement agencies with the approval of the Additional Director of the Group. Additional information can also be requested from foreign FIUs for further processing of STRs with the approval of the Director of the FIU-IND.

289. Individual CTRs are not analysed as such but the information contained in these reports is used to support the analysis of STRs and to respond to information requests. During the financial year 2008-2009, the CTR data were processed to generate clusters of CTRs on the basis of direct and indirect relationships.

Certain high-risk clusters were analysed and disseminated as CTR analysis reports to the Directorate of Enforcement, the Central Board of Direct Taxes, and Intelligence agencies.

Dissemination of Information

290. Section 66(1) of the PMLA provides that the Director of the FIU-IND or any other authority specified by the Director may disseminate any information received by the FIU under that Act to any tax authorities or enforcement agencies involved with the prevention of illicit traffic in narcotic or psychotropic substances under the NDPS Act. In addition, pursuant to section 66(2), such information may also be provided to any person specified by notification in the Official Gazette, and through the Government Notifications G.S.R.381(E) respectively G.S.R 929(E), the following other law enforcement and intelligence agencies were identified as authorities to which the FIU can disseminate information:

- a. the Directorate of Enforcement under the Ministry of Finance, Department of Revenue;
- b. the Cabinet Secretariat (Research and Analysis Wing);
- c. the Ministry of Home Affairs or National Security Council Secretariat or Intelligence Bureau;
- d. the Economic Offences Wing of the Central Bureau of Investigation;
- e. the Chief Secretaries of the State Governments²⁶;
- f. the Reserve Bank of India;
- g. the Department of Company Affairs, Government of India;
- h. the Securities and Exchange Board of India;
- i. the Insurance Regulatory and Development Authority of India.
- j. the Central Economic Intelligence Bureau (CEIB);
- k. the Serious Fraud Investigation Office (SFIO); and
- l. the National Investigation Agency (NIA).

291. The FIU-IND also receives requests from law enforcement agencies, including requests to source information from foreign FIUs through the Egmont Group. Requests of this nature are transmitted to the foreign FIU noting that it is on behalf of a law enforcement agency and specific authority to provide the information to that requesting authority is always obtained in line with the Egmont Group guidance on this.

292. After processing the STR, the Additional Director and relevant senior technical officers (the Committee) decide whether the STR needs to be disseminated outside the FIU or retained within the FIU. The decision regarding which agency the STR should be disseminated to is based on the following factors:

- a. the type of suspicion reported in the STR;
- b. the nature of the suspected offence;
- c. the transaction pattern in the STR;
- d. the linkage with other STRs, CTRs and CDFs;
- e. the transaction pattern in linked CTRs;

²⁶

The Chief Secretaries of a State is the head of all Departments, including the Police Department in the State. In actual practice, the Chief Secretaries have nominated a senior Police Officer as the "PMLA Nodal Officer" to receive information from the FIU on his behalf. This ensures effective dissemination, action and reporting back.

- f. the linkage with earlier related references received from other agencies; and
- g. the linkage with other lists maintained at the FIU-IND.

293. The decision whether or not to disseminate STRs is taken and recorded in the form of draft minutes which are signed by all the members of the Committee. The decision of the Committee is reviewed on a selective basis by the Director of the FIU-IND. After review, the minutes are countersigned by the Director of the FIU-IND and formally issued.

294. During the course of processing, significant cases are categorised separately as category-A. Approximately 3-5% of disseminations relate to category-A files and these relate to matters where a high level of predicate offence is suspected. In these circumstances the approval of the Director of the FIU-IND needs to be obtained before dissemination of category-A STRs can take place.

Protection of Information

295. Information is disseminated only to the authorities referred to in section 66(1) of the PMLA and to authorities notified by the Central Government under section 66(2) of the PMLA (see above). Section 5 of the Official Secrets Act provides for punishment with imprisonment for a term which may extend to three years, or a fine, or both if a person, who has in his possession any information which he has obtained or to which he has access owing to the position he holds under the Government, wilfully communicates the information to any person other than the person to whom he is authorised to communicate it or fails to take reasonable care of the information.

296. The FIU-IND has also taken physical and information security measures to ensure proper use of the information. A layered security approach has been adopted by the FIU-IND to address the physical environment and personnel, as well as the areas specifically related to safeguarding information. This includes electronic access controls, biometric access control, video monitoring, personnel identification, separation of areas, etc. These controls are put in layers and complement each other. They also complement the information security measures. In this regard, The implemented information security instructions covering information classification, internet usage, Minimum Baseline Security Standards (MBSS), password protection, operational security, media security, virus management and incident reporting. Moreover, the FIU-IND is currently enhancing its IT security architecture and a specific security policy, based on the ISO/IEC27002:2005 code of practice for establishing, implementing, operating, monitoring, reviewing maintaining and improving information security, has been developed. The assessment team is of the view that the information held by the FIU-IND is securely protected;

FIU Guidance and periodic reports

297. On 1 July 2005, the Central Government of India issued its Notification GSR.444(E) regarding The Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (referred to as the PML Rules). Rule 7(4) requires every banking company, financial institution and intermediary to observe the procedure and the manner of furnishing information as specified by the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority (IRDA).

298. The reporting formats and the procedure and manner for submitting STRs and CTRs have been finalised by the regulators in active consultation with the FIU-IND. The FIU-IND provides report preparation utilities to assist reporting entities in preparation of the reports in electronic form but also provides guidance to assist the reporting entities who do not have the technical capability to generate

reports in electronic form. The reporting formats and utilities can be downloaded from the FIU's website (<http://fiuindia.gov.in>).

299. The FIU-IND has also published various brochures such as Obligations of Entities in Financial Sectors under Prevention of Money Laundering Act; How to Report Cash Transactions; and How to Detect and Report Suspicious Transactions. The FIU and Regulators are providing financial institutions and other reporting parties with interactive guidance regarding the manner of reporting and the procedures that should be followed when reporting through seminars and training workshops, and review meetings with principal officers of reporting entities (see detailed discussion in Section 3.7 below). In addition, an annual Train the Trainers workshop is organised by the FIU-IND with the objective to increase the expertise of master trainers of major reporting entities engaged in imparting in-house AML/CFT training in their organisations.

300. Since 2007, the FIU-IND has publicly released an annual report which contains information on the organisation, the initiatives taken to strengthen its capacity, statistics, and examples of suspicious transactions reported by various reporting entities, however, the report does not contain a specific section on typologies and trends. The annual report is available on the FIU's website. The website also contains a range of additional information, including responses to frequently asked questions, relating to AML/CFT and the role of the FIU. The FIU also periodically publishes an FIU newsletter (FINnews) providing information to reporting entities.

Egmont Group membership and international exchange of information

301. In May 2007 the FIU-IND became a member of the Egmont Group and actively participates in the various Egmont working groups. The FIU-IND can exchange information without an MOU and in practice; it exchanges information on the basis of confidentiality and reciprocity, as foreseen in the Egmont Principles for Information Exchange between Financial Intelligence Units (see also Section 6.5 of this report). Over the three years of operation, the FIU has received 173 requests from foreign FIUs and has in turn made 46 requests to foreign FIUs for information, involving 65 separate countries. The FIU-IND also shares information with counterparts that are not members of the Egmont Group.

302. Although the FIU-IND is able to interact with foreign FIUs without an MOU, it has taken a proactive approach in signing MOUs with other FIUs, especially with countries that require signing of MOUs for exchange of information. As of December 2009, the FIU-IND had signed MOUs for sharing of information with counterpart foreign FIUs in seven countries, namely Mauritius; Philippines; Brazil; Malaysia; Russia; Australia and Canada. The FIU-IND has been regularly exchanging information with foreign FIUs over the Egmont Secure Web (ESW) and has put in place a mechanism to respond to requests from foreign FIUs in a timely manner.

Recommendation 30 - Structure, funding, human and technical resources (FIU)

Adequately structured, sufficient funding, technical and other resources

303. The FIU-IND appears to be well structured for its task with independence in terms of its reporting and co-ordination. At the time of the on-site visit, the FIU-IND had an overall strength of 43 staff, but had a current strength of 36, with seven unfilled positions. The Indian Government recently decided to further strengthen the FIU-IND's human resources. Early 2010, 31 additional posts were created at various levels within the FIU through a Government Order dated 9 February 2010. The total personnel strength of the FIU-IND has so been raised from 43 posts to 74 posts. Steps have been initiated to hire persons for the already vacant and recently created new positions.

304. As indicated above, the FIU staff is divided into six groups, comprising an Additional Director, senior technical staff and support staff, and each of these groups has a wide range of sector and functional

responsibilities. In addition to the designated groups, the Information Technology (IT) related work is handled by the Technical Director and the technical team and a separate Administration section functions under the supervision of an Additional Director which handles all work related to administration, budget, accounts and general administration. In addition, the FIU-IND receives IT support from the Ministry of Information Technology.

305. The FIU-IND uses specialised hardware and software for importing, validating and processing data. It has initiated the project FINnet (Financial Intelligence Network), with the objective to adopt industry best practices and appropriate technology to collect, analyse and disseminate valuable financial information for combating money laundering and related crimes. The project would cover key processes of intelligence management, relationship management, strategic management, resource management and technology management.

Professional standards, skills and confidentiality of staff

306. The FIU-IND is headed by the Director, an Indian Administrative Service (IAS) officer at the level of Joint Secretary to the Government of India. The FIU-IND is manned by persons drawn, after proper scrutiny, from various government departments and agencies including the Indian Revenue Service (IRS), the RBI, and others. They are governed by their respective conduct rules and regulations and the Official Secrets Act, which address issues of confidentiality, expectations of professional standards and integrity.

Training for FIU staff in combating ML and FT

307. The FIU-IND trains its employees in-house as well as through various domestic and international/bilateral training programmes on AML/CFT to allow them to perform their functions in an effective manner. The FIU-IND staff have visited the FIUs of Australia, Canada and the USA to learn from their functioning. In addition, officers of the organisation have attended training programmes and workshops on AML/CFT issues in India, Thailand, Singapore, Indonesia, Sri Lanka, and other countries to enhance their skills in various areas of work relating to the FIU. The officers of the FIU-IND regularly attend working group meetings and typologies workshops organised by the Egmont Group, the FATF and the APG.

Recommendation 32 (FIU) - Statistics

308. The FIU-IND maintains statistics on the receipt, analysis and dissemination of STRs along with breakdowns of the type of financial institution submitting the report and the agencies to which information is disseminated. Some of these statistics can be found in the discussion of the STR and CTR reporting in Section 3.7 below.

Statistics: Receipt of Suspicious Transaction Reports (STRs)

| Category | 2006-2007 | 2007-2008 | 2008-2009 | Up to December 2009 | Total |
|------------------------|------------|--------------|--------------|---------------------|---------------|
| Banks | 437 | 1 183 | 2 826 | 4 048 | 8 494 |
| Financial Institutions | 88 | 288 | 841 | 989 | 2 206 |
| Intermediaries | 292 | 445 | 742 | 819 | 2 298 |
| Total | 817 | 1 916 | 4 409 | 5 856 | 12 998 |

Statistics: Analysis of STRs

| | 2006-2007 | 2007-2008 | 2008-2009 | Up to December 2009 | Total |
|--------------|-----------|-----------|-----------|---------------------|--------|
| STR Received | 817 | 1 916 | 4 409 | 5 856 | 12 998 |
| Processed | 646 | 2 001 | 4 019 | 5 120 | 11 786 |
| Disseminated | 391 | 935 | 2 270 | 3 154 | 6 750 |

Statistics: Dissemination of STRs²⁷

| | 2006-2007 | 2007-2008 | 2008-2009 | Up to December 2009 | Total |
|--------------------------|------------|------------|--------------|---------------------|--------------|
| Law Enforcement Agencies | 338 | 885 | 2 319 | 3 115 | 6 657 |
| Intelligence Agencies | 60 | 49 | 90 | 103 | 302 |
| Regulators & others | 30 | 34 | 41 | 90 | 195 |
| Total | 428 | 968 | 2 450 | 3 308 | 7 154 |

Table: Details of STRs disseminated to various agencies

| Agency | 2006-2007 | 2007-2008 | 2008-2009 | Up to December 2009 | Total |
|--|------------|------------|--------------|---------------------|--------------|
| Directorate of Enforcement (ED) | 35 | 68 | 90 | 132 | 325 |
| Central Board of Direct Taxes (CBDT) | 254 | 677 | 1766 | 2 520 | 5 217 |
| Central Board of Excise and Customs (CBEC), Directorate of Revenue Intelligence (DRI) and Directorate General of Central Excise Intelligence (DGCEI) | 10 | 14 | 26 | 27 | 77 |
| Narcotics Control Bureau (NCB) | 3 | 2 | 1 | 15 | 21 |
| Ministry of Home Affairs (MHA) and Intelligence Agencies | 58 | 51 | 97 | 104 | 310 |
| Ministry of Company Affairs (MCA), Serious Fraud Investigation Office (SFIO) | 6 | | 5 | 5 | 16 |
| Central Bureau of Investigation (CBI) | 24 | 83 | 46 | 37 | 190 |
| State Governments | 12 | 42 | 378 | 413 | 845 |
| Reserve Bank of India (RBI) | 1 | 2 | 5 | 15 | 23 |
| Securities and Exchange Board of India (SEBI) | 27 | 35 | 30 | 47 | 139 |
| Insurance Regulatory and Development Authority of India (IRDA) | | 1 | 6 | 4 | 11 |
| Others | | 6 | 4 | 3 | 13 |
| Total | 430 | 981 | 2 454 | 3 322 | 7 187 |

²⁷

The total numbers of STRs disseminated in this table differentiate from the numbers included in the table above for the following reason: STRs processed but not disseminated in a previous year may be disseminated in one of the following years based on a request from domestic law enforcement and intelligence agencies, foreign FIUs or other information or new intelligence received that justifies the dissemination.

Additional elements

309. Statistical information relating to the number of investigations, prosecutions or convictions for ML, FT or underlying predicate offences that were initiated through the dissemination of FIU information was not available, but the FIU-IND did provide information in relation to specific cases that it had contributed to. In addition, a number of government agencies had published in their annual report commentary on their interaction with the FIU-IND that included reference to various case studies.

Implementation and effectiveness

310. Given that the FIU is a stand-alone agency it carries within its strength of 43 personnel a number of administrative and information technology support staff. Taking into account the number of staff involved in supporting the FIU, and also that at the time of the on-site visit the FIU had seven vacancies, the number of staff in the FIU involved in carrying out the analytical role of the FIU is at a bare minimum in terms of maintaining effectiveness. The staffing level within the FIU during the on-site visit in December 2009 was such as to raise a concern as to whether this was sufficient to meet the expected increase in STR reporting in the 2009–2010 year. However, Indian authorities advised the assessment team that an additional 31 posts were created at various levels within the FIU through a Government Order issued on 9 February 2010. The total authorised personnel strength of the FIU-IND has therefore been raised from 43 posts to 74 posts. Indian authorities further advised that steps have been initiated to hire persons for the already vacant and recently created new positions.

311. The State Police have a number in excess of one million staff and have primary responsibility for the investigation and prosecution of FT and predicate offences to money laundering, and also for confiscation of proceeds of crime. The overall scale of offending and also the number of criminal investigations (estimated that six million proceedings are presently before the criminal courts) in India is very large. However, taking into account the scale of the Indian system, the number of disseminations by the FIU-IND to the State Government (and thereby to the State Police) is limited when compared, for example, with the number of disseminations to tax and revenue agencies. This then impacts on the overall effectiveness of the FIU in terms of its dissemination of financial information for investigation or action by the State Police. The FIU-IND should identify the reasons why the level of disseminations to the State Government is relatively low in comparison with the percentage of disseminations to other competent authorities and agencies in order to ensure that it provides effective financial intelligence to the State Police for the investigation and prosecution of terrorist financing, ML predicate offences, and confiscation (e.g. is there a need to improve its access to Police intelligence or to enhance the FIU's understanding of Police intelligence requirements). Once the reasons have been identified, the FIU should give due consideration to taking the necessary steps to address the possible deficiencies in its STR processing and analysis systems, including the dissemination of information, in order to enhance the FIU's ability to better meet the intelligence needs for serious crime investigations.

312. Public information released from the FIU-IND should be extended to also cover typologies information and trends in ML and FT cases, which could include strategic analysis, to better enable reporting entities to meet their obligations in terms of AML/CFT risks.

2.5.2 Recommendations and Comments

313. It is recommended that the FIU-IND:

- Should enhance its capability in relation to intelligence and information dissemination to all competent authorities, including the State Police.
- Should enhance its dissemination of public information regarding trends and typologies, which could include strategic reporting.

2.5.3 Compliance with Recommendation 26

| | Rating | Summary of factors relevant to s.2.5 underlying overall rating |
|------|--------|---|
| R.26 | LC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ the dissemination of financial information for investigation or action by the State Police is relatively low in comparison with the State Police's primary responsibility for the investigation and prosecution of FT and predicate offences to money laundering, and for confiscation of proceeds of crime. • Public information released by the FIU-IND does not include information on typologies and trends in ML and FT cases and related predicate offences. |

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R. 27 & 28)

2.6.1 Description and Analysis

Recommendation 27 (Designated law enforcement authorities)

314. India's law enforcement framework is structured according to the respective federal and state responsibilities of agencies involved in the investigation and prosecution of money laundering, terrorist financing, and predicate offences. Therefore, according to the VIIth Schedule of the Constitution of India, "Public Order is the State subject". State Police forces with in excess of one million police personnel are responsible for the investigation of all public order and criminal matters, including predicate offending and FT matters. Under the Constitution there is no authority to establish a federal police agency.

315. In relation to the investigation and prosecution of money laundering, Chapter III of the Prevention of Money Laundering Act (PMLA) regarding Attachment, Adjudication and Confiscation establishes the statutory framework for the confiscation of proceeds of ML related offences and similarly, Chapter V of the PMLA regarding Summons, Searches and Seizures sets out investigative powers for the purpose of investigating incidents of suspected ML offences. As with the FIU-IND, Chapter VIII of the PMLA regarding Authorities provides for the appointment of specified Authorities for the purposes of the PMLA, and section 49 states that the Central Government may appoint such persons as it thinks fit for the purposes of being Authorities under the PMLA.

316. On 1 July 2005, the Government of India published in the Gazette of India a notification (reference: G.S.R.No.440(E)) appointing the Director of Enforcement as the Director with exclusive powers for the purpose of the investigation of ML offences. No other agency in India may exercise jurisdiction under the PMLA for the purpose of carrying out a ML related investigation. Locating responsibility for money laundering within the Directorate of Enforcement (ED), which is a federal enforcement agency, highlights the perspective that fiscal security underscores that agency's mandate to investigate this type of offending.

317. In relation to the investigation and prosecution of FT offences, while these are essentially investigated by the State Police, the Unlawful Activities (Prevention) Act (UAPA s.43) also empowers the Central Bureau of Investigation (CBI), constituted under the Delhi Special Police Establishment Act, 1946 to investigate FT offences. In addition, the Central Government has constituted under the National Investigation Agency Act (NIA Act), 2008 the National Investigation Agency (NIA), a specialised agency for the investigation and prosecution of offences under the Acts mentioned in the schedule to the NIA Act, including the UAPA. At the time of the on-site visit, the NIA was investigating three FT related cases.

318. In practice, the State Police would start a FT investigation and where this unfolds as a complicated or complex investigation or has multiple linkages then the State Police can pass this investigation on to the CBI or the NIA, which will continue the investigation. The Central Government has powers to assign cases relating to offences specified in the schedule to the NIA Act, *suo-motu*.

Postponement of Arrest and/or Seizure of Money

319. Based on Chapter V of the PMLA (ss.16-20), the investigation officers are empowered with the power of survey, search and seizure, search of persons and arrest, if there is reason to believe that a ML offence has been committed. The Indian authorities state that the word “may” in the respective sections gives sufficient discretion to the investigating officer to postpone or waive the arrest of suspected persons and/or the seizure of the money taking into account the interest to the investigation conducted on the basis of the PMLA. So far, no case under investigation under the PMLA has warranted such action. In practice, investigating officers postpone the arrest of a suspected person in order to identify other persons involved or to gather further evidence.

Additional elements

Special investigative techniques

320. Special investigative techniques for conducting investigations relating to ML or FT offences are available such as surveillance of the suspected persons, discreet enquiries, wire tapping and the interception of private communications for the collection of evidence. The (Indian) Telegraph Act, 1885 empowers both state and federal agencies to intercept telecommunications, under certain circumstances, with the approval of the competent authority. The Indian authorities state that such techniques are used depending on the facts and circumstances of the case under investigation. In addition, the authorities state that the use of such techniques has enabled authorities to successfully investigate a number of cases. ML and FT case examples demonstrating special investigation techniques were provided to the evaluation team during the on-site visit. It should be noted, however, that the PMLA does not contain a specific provision to undertake controlled deliveries.

Special investigative Groups

321. The Indian authorities state that having regard to the facts and circumstances of each case, the gravity of the offence and the magnitude of the evidence which is required to be collected, temporary groups specialised in the investigation of proceeds of crime are being formed for financial investigations. The mandate of such a temporary group is to carry out investigations under the PMLA that may entail seizure, attachment and confiscation of the proceeds of crime.

322. The PMLA provides for co-operation between India and any requesting State for the investigation of ML offences through the mutual legal assistance provisions provided in Chapter IX of the PMLA. In addition, pursuant to letter F.No.16/50/2006-Ad.Ed dated 21 April 2008, the Director of Enforcement has been authorised to grant permission, when necessary, for the presence of foreign officers/investigators in India after grant of administrative approval from the DOR for execution of an inbound request for mutual legal assistance. Joint investigations with foreign law enforcement agencies do take place. During these investigations special investigation techniques are applied, if required.

Typologies and sharing of information amongst agencies

323. The various law enforcement agencies engaged in AML and CFT actions meet periodically in different multi-agency fora and review ML/FT methods, techniques and trends (see Section 6.1 for more details). The results of the analyses are presented in the form of reports that are circulated among the agencies concerned.

324. At the national level, the Economic Intelligence Council (EIC) headed by the Finance Minister reviews the effectiveness of ML and FT measures. The Central Economic Intelligence Bureau (CEIB) undertakes a quarterly review through the Regional Economic Intelligence Councils (REICs) while the FIU-IND does a regular review of the ML and FT trends and techniques based on the results of its own analysis and the feedback it receives from the investigative agencies following its dissemination of information. Finally, the DOR reviews the outcomes of ML and FT investigations by various agencies as an ongoing process. The Indian authorities state that at least three types of actions are taken on the basis of such reviews. Firstly, amendments to the legal basis or operational instructions, wherever required; secondly, remedial administrative action regarding resources, including steps to expedite appointments; and thirdly, improving inter-agency co-ordination and co-operation by strengthening existing mechanisms or instituting new mechanisms such as increased use of IT for analytical purposes.

Recommendation 28 (investigative powers)

Powers of production, search and seizure

325. Section 50 of the PMLA provides the officers of the Directorate of Enforcement (ED) when investigating ML offences with the same powers as are vested in a civil court under the Code of Criminal Procedure (CrPC) in respect of the following matters, namely:

- a. discovery and inspection;
- b. enforcing the attendance of any person, including any officer of a banking company or a financial institution or a company, and examining him on oath;
- c. compelling the production of records;
- d. receiving evidence on affidavits;
- e. issuing commissions for examination of witnesses and documents; and
- f. any other matter which may be prescribed.

326. The officers of the ED are also empowered to search persons or premises for, and seize transaction records, identification data, account files and business correspondence, and other records or documents (PMLA ss.17-18).

327. The UAPA (s.43(C)) and the NIA Act (s.3) provide that the provisions contained in the CrPC regarding the powers to arrest, search for and compel production are also applicable for the investigation of FT offences. Based on these provisions, the investigating officer can compel the production of documents; search persons or premises for documents, records and information; and seize certain property (ss. 91, 93, 102 and 165 of the CrPC). In addition, the investigating officer may require any officer or authority of the Central Government and State Government, a local authority, a bank, a company, a firm or any other institution, establishment, organisation or any individual to furnish the information in his or its possession in relation to the offence, where the investigating officer has reason to believe that such information will be useful for or relevant to the investigation (UAPA s.43F(1)). Further, section 43A of the UAPA empowers designated authorities to search for records, documents, etc. under certain circumstances.

Powers to take witness statements

328. Section 50 of the PMLA read with Notification G.S.R. 440(E) issued on 1 July 2005 empowers the officers of the ED in charge of the investigation of ML offences to summon any person whose attendance is considered necessary to give evidence during the course of any investigation or proceedings under the Act. All persons so summoned shall be bound to attend in person or through authorised agents, as the investigating officer directs, and shall be bound to state the truth upon any subject respecting which they are examining or making statement. Section 50 further provides that these proceedings shall be

deemed to be a judicial proceeding within the meaning of section 193 (Punishment for false evidence) and section 228 (Intentional insult or interruption to a public servant sitting in judicial proceeding) of the Indian Penal Code (IPC). The ED advised that statements compelled from suspects may still be used in criminal proceedings (CrPC s.161 and Evidence Act s.80), and that this contrasts with the restrictions on the use of such statements taken from suspects by the Police, which are not admissible unless the witness gives contrary evidence.

329. The State Police authorities, the CBI and the NIA, who are entrusted with the responsibility of investigating FT offences, have the power to take witnesses' statements for use in investigation and prosecution of FT and underlying predicate offences. The relevant provisions exist in sections 160 and 161 of the CrPC and are made applicable to investigations under the UAPA (s.43(C)) and the NIA Act (s.3). In addition, under section 31 of the UAPA, the designated authorities exercising powers under Chapter V (forfeiture of proceeds of terrorism) have been vested with the powers of a civil court for the purpose of making a full and fair enquiry into the matter.

Recommendation 30 - Structure, funding, human and technical resources (Law enforcement authorities)

The Directorate of Enforcement (ED)

330. The ED was established in 1956 and is an intelligence and investigative arm of the Central Government. It has a pan-Indian character, with 21 field offices spread over various States and Regions in India (see also Section 1 for more details regarding the role of the ED in general). With an officer in the rank of Additional/Special Secretary to the Government of India as its Head, the Directorate has, as the core team for undertaking the anti-money laundering function, three Special Directors of Enforcement at the level of Joint Secretary to the Government of India; two Additional Directors; 12 Deputy Directors of Enforcement; and 74 Assistant Directors. The officers are either directly recruited or drawn from the country's civil services such as the Indian Administrative Services, the Indian Revenue Services and the Indian Police Services. The overall staff strength of the Directorate is 745, including secretarial/ministerial and other support staff, as indicated in the table below:

| | Post | Sanctioned Strength |
|-----|--|----------------------------|
| 1. | Director of Enforcement | 1 |
| 2. | Special Director of Enforcement | 3 |
| 3. | Additional Director | 1 |
| 4. | Additional Director (Prosecution) | 1 |
| 5. | Deputy Director | 12 |
| 6. | Deputy Legal Adviser | 2 |
| 7. | Assistant Legal Adviser | 10 |
| 8. | Assistant Director | 74 |
| 9. | Enforcement Officers & Assistant Enforcement Officers | 240 |
| 10. | Superintendent and other ministerial/secretarial staff | 261 |
| 11. | Other support staff | 140 |
| | Total | 745 |

331. The ED is enforcing the Prevention of Money Laundering Act (PMLA), the Foreign Exchange Management Act (FEMA), and is one of the agencies enforcing the Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974 (COFEPOSA). The evaluation team was informed that of these three statutory roles, the investigation of ML offences is the principal priority for the ED and that the majority of that agency's 745 staff are being directed towards ML investigations. The ED receives information from a range of sources regarding ML predicate offending, then decides upon its own priorities for the investigation of the ML component to this offending. Securing proceeds of the offending and collection of evidence are the two key responses, which are then followed by the prosecution process. The ED has 21 field offices, with 10 zonal offices headed by Deputy Directors, and 11 offices headed by Assistant Directors. Each field office liaises directly with the State Police and other law enforcement agencies – for example the Punjab office of the ED has 40 staff who work closely with the State Police across the full range of ML predicate offence types and investigations. The following table provides a breakdown of the predicate offence types for the 798 investigations registered by the ED.

| Offences | before 01.06.2009 | after 01.06.2009 | TOTAL |
|--------------------------------------|-------------------|------------------|-------|
| NDPS Act | 15 | 292 | 307 |
| Indian Penal Code (IPC) | 45 | 354 | 399 |
| Prevention of Corruption Act | 1 | 52 | 53 |
| Unlawful Activities (Prevention) Act | - | 18 | 18 |
| Wild Life (Protection) Act | 2 | 5 | 7 |
| Passports Act | - | 5 | 5 |
| Arms Act | 1 | 4 | 5 |
| Explosive Substances Act | - | 3 | 3 |
| Customs Act | - | 1 | 1 |
| TOTAL | 64 | 734 | 798 |

332. The ED has initiated an IT programme for use at various stages of investigation and further action in PMLA cases. Customised software has been developed for storage of data and online access by various levels of officers in the organisation. Authorised officers can upload documents in the matters pertaining to their specified jurisdictions or use a search engine to scan through uploaded documents. This browser based software allows for work flow management in respect of the PMLA cases dealt with by the Directorate.

333. During the financial year 2009-2010, the Directorate has an Annual Budgetary Grant of INR 514.20 million (USD 10.284 million), which includes provision for the further development and maintenance of the IT programme and for hiring legal and other professional experts.

334. Officers and personnel in the ED are recruited through a selection process to ensure that they possess the necessary knowledge and professional and integrity/confidentiality standards. Whereas almost

half of the officers are directly recruited into the Directorate through various public selection boards, the remaining are inducted on secondment from various law enforcement agencies.

335. Specialised AML/CFT training courses are being periodically organised for the officers of the ED at various training centres, including those of the CBI, the Central Board of Excise and Customs (CBEC), the Central Board of Direct Taxes (CBDT), and the Indian Law Institutes. Also, a number of officers at various levels have attended courses/seminars arranged by the United Nations, the World Bank, the APG, and others, both in India and in other countries. The employees of the ED have also attended training in Singapore, Sri Lanka, Thailand, and the USA in view of enhancing their professional skills in the field of investigations and further action under the AML/CFT framework.

The Central Bureau of Investigation (CBI)

336. The CBI is the Central Police Agency to investigate cases of bribery and corruption, violation of Central fiscal laws, major frauds relating to the Government of India departments, public sector companies, passport frauds, cyber crimes and serious crimes committed by organised gangs and professional criminals – the CBI does not have a mandate to investigate ML offences, but liaises directly with the ED through designated *nodal* officers for this purpose. The CBI has a sanctioned strength of 5 961 officers, including 4 078 Executive (Investigation) officers involved in various investigations; 230 Legal (Prosecution and Legal Advice) Officers; 155 technical officers; and 1 428 support staff. The Directorate of Prosecution in the CBI is responsible for conducting and supervising the criminal cases pending trial, appeal and revision in the courts.

337. The CBI academy has conducted 5 training courses between 2005 and January 2009 on the subject of “investigation under the PMLA” which was attended by 114 officers of which 42 were from the State police. The CBI’s training infrastructure has further been expanded with the establishment of three regional training centres which have been equipped with modern training aids with an aim to maximise training outcome in a cost effective manner.

The State Police

338. In the States, the police authorities are the investigating agencies for predicate offences and FT offences, and this includes crimes associated with terrorist attacks in India. Many States have constituted specialist squads, including organised crime, economic crime, and terrorism related investigative groups. Various case studies were provided by the State Police during the on-site visit to demonstrate investigative capability, and inter-agency co-ordination and co-operation. Each State has a separate prosecution wing with Senior Public Prosecutors, Special Prosecutors and Assistant Public Prosecutors. The respective State Police forces are headed by the Director-General of Police. In the district, the Police are headed by a Senior Superintendent of Police or a Superintendent of Police, who supervises the work relating to investigations and policing. The Deputy Inspectors General supervise the Superintendents of Police and are in turn supervised by the Inspectors General. The State Police are assisted by legal and prosecution experts at every level. They are funded by the respective State Governments and are also provided assistance by the Central Government in terms of equipment, training, sharing of intelligence, and capacity building.

339. Apart from the training opportunities in the CBI described above, police officers from the State Police also receive training to update their skills at the National Police Academy, and in various other police training schools located in different States, with an emphasis on investigation skills. The CBI has organised workshops with a special focus on capacity building of the State Police to improve the investigation techniques.

The National Investigation Agency (NIA)

340. The NIA is headed by the Director General and there are 217 posts at various levels, which include officers at the level of Additional Director General, Inspectors General, Deputy Inspectors General, and Superintendents of Police. The NIA also has legal officers at the level of Additional Legal Adviser, Senior Public Prosecutor, Public Prosecutor, and others. The NIA's role is to focus on the investigation of FT offences, it does not extend to ML offences but nevertheless, the NIA works closely with the ED in relation to ML predicate offences, through its network of *nodal* officers.

341. More generally, the Indian authorities advise that the officers and staff of the law enforcement/investigative agencies are given adequate training, which also includes familiarisation with the latest ways and means being adopted by terrorists and terrorist organisations for raising, collecting, providing funds for terrorist activities and the measures required to combat terrorist financing.

Recommendation 32 – Statistics and effectiveness

342. In the period to June 2009 the number of ML investigations was all but non-existent, with just two proceedings having been commenced in relation to ML offences and no convictions. However, the evaluation team were advised that two key legislative changes in 2009 have cleared the way for the ED to increase significantly the number of active ML investigations and therefore, the effectiveness of its enforcement of ML offences: firstly, the scope of offences that are included as predicate offences for ML was extended, and secondly, the requirement for a charge to have been laid for the predicate offence before the ED was able to commence a ML investigation was amended – the ED may now commence an investigation without the requirement for charges to have been laid for the predicate offence. On 31 December 2009, a total of 798 investigations were registered, including 43 cases involving provisional restraining of proceeds of crime. The total sum of restrained property was INR 3 billion (USD 60 million), which includes some very large, high profile individual cases. The ED demonstrated effective investigative powers and capability.

343. The approach in India to ML investigations, whereby the one agency (being the ED) has sole jurisdiction, is an unusual approach that risks preventing a more mainstream response to ML from a wider group of law enforcement agencies. However, indications from information provided to the evaluation team, including the overall number of investigations now underway, the combined value of assets restrained, and various individual case examples, suggest that sole jurisdiction within the ED will ensure that ML offences are properly investigated in India.

2.6.2 Recommendations and Comments

344. While India has initiated a large number of ML investigations, it has yet to achieve convictions for ML offences.

2.6.3 Compliance with Recommendations 27 and 28

| | Rating | Summary of factors relevant to s.2.6 underlying overall rating |
|------|--------|--|
| R.27 | LC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ India has yet to achieve ML convictions. |
| R.28 | C | This Recommendation is fully observed. |

2.7 *Cross Border Declaration or Disclosure (SR.IX)*

2.7.1 *Description and Analysis*

Special Recommendation IX

345. To implement SR IX, India uses a combination of a declaration system (pursuant to the Foreign Exchange Management Act) by using Currency Declaration Forms (CDFs) and a disclosure system. Customs officers are empowered to enforce the restrictions placed by the Government on the import and export of currency (FEMA s.38). The declaration and disclosure regimes (as explained below) apply to currency and BNI carried by incoming persons both via India's airports and land borders. There are restrictions on sending currency and BNI and outgoing to and from India through post and cargo.

Declaration system for incoming persons

346. India has legal controls on physical cross border transportation of currency and bearer negotiable instruments (BNI) through the Foreign Exchange Management Act, 1999 (FEMA) and the Foreign Exchange Management (Export and Import of Currency) Regulations, 2000 (the Regulations), which were issued by the RBI based on section 6(3)(g) of the FEMA. The FEMA was implemented as an Act with the objective of facilitating external trade and payments and for promoting the orderly development and maintenance of the foreign exchange market in India. While not designed for this purpose, the controls on the physical cross border transportation of currency and BNIs is also used for AML and CFT purposes.

Import of foreign exchange into India

347. There is a general provision in Clause 5 of the Regulations that prohibits a person, without the general or special permission of the RBI, to export or send out of India or to import or bring into India any foreign currency. However, pursuant to Clause 6 of the Regulations a person is permitted to send or bring currency into India on the condition that either:

- a. the aggregate value of the foreign exchange in the form of currency notes, bank notes or traveller's cheques brought in by such person at any one time does not exceed USD 10 000 or its equivalent and/or the aggregate value of foreign currency notes brought in by such person at any one time does not exceed USD 5 000 or its equivalent; or
- b. this person makes, on arrival in India, a declaration to the customs authorities in the Currency Declaration Form (CDF) annexed to the Regulations.

348. The term "Currency" is defined to include all currency notes, postal notes, postal orders, money orders, cheques, drafts, traveller's cheques, letters of credit, bills of exchange and promissory notes, credit cards or such other similar instruments, as may be notified by the RBI. Currency notes include cash in the form of coins and bank notes (FEMA ss.2(h) and (i)).

349. India shares its land borders with Pakistan, Nepal, Bhutan, Bangladesh, Myanmar, China and Afghanistan. Along these borders, there are 78 Land Customs Stations (LCS) declared under section 7 of the Customs Act. Passengers crossing the land borders into or out of India do so through the LCS. The Indian authorities advised the assessment team that the Currency Declaration Form is applicable to incoming passengers who carry currency beyond the prescribed threshold, and that the declaration is recorded in the relevant register and dated signature of the passenger obtained.

Disclosure system for outgoing persons***Export of Foreign Exchange***

350. Clause 7 of the Regulations gives an overview of the circumstances in which an authorised person or any other person may take or send currency and BNI out of India. Contrary to the import of foreign exchange, there is no declaration obligation attached to the export of foreign exchange. However, the Indian authorities state that given the fact that the export of foreign exchange is only permitted in specific circumstances, the customs authorities have the authority to make inquiries on a targeted basis, based on intelligence or suspicion, and that in such circumstances a disclosure obligation applies.

Indian currency and currency notes

351. Clause 3 of the Regulations gives an overview of the circumstances in which any person resident in India may take or send outside India Indian currency and currency notes. No declaration obligation is attached to this, but in relation to the export of Indian currency, the Indian authorities state that the disclosure obligation also applies when customs officers make inquiries based on intelligence or suspicion.

Transportation through mail and containerised cargo

352. Transportation through mail and containerised cargo is prohibited by law. However, an Authorised Person²⁸ licensed by the RBI may send currency and BNI into or outside India through mail and containerised cargo but is under the obligation to file a report to Customs in this regard.

Powers to obtain further information

353. The Central Government has empowered customs officers to enforce the restrictions placed by the RBI on the import and export of currency (FEMA s.38). A failure to file a currency declaration form upon entry to India or to disclose the carriage of currency out of India will amount to a breach of the Customs Act (ss.111 or 113) and will give rise to a power by customs officers to request and obtain further information with regard to the origin of the currency and its intended use upon discovery of a false declaration (Customs Act s.107).

354. The customs authorities also state that, at present, when a passenger declares currency more than USD 5 000 or equivalent, discreet profiling and questioning of the passenger is carried out by the customs officer with respect to the purpose of the visit of the passenger, their profession, and the purpose for which the foreign currency is being brought into the country in view of detecting false declarations.

355. The assessment team received no information about specific actions taken by India to detect unauthorised transportation of currency and BNI through mail and containerised cargo and this lead the team to conclude that no such actions are therefore taken.

Power to stop and restrain goods, and apply provisional measures and confiscation***Suspicion of money laundering or terrorist financing***

356. In cases where there is a suspicion of money laundering, the customs authorities would alert the officers of the Directorate of Enforcement (ED) for necessary action under the PMLA, including attachment/seizure of the proceeds of crime. However, in cases of a suspicion of money laundering or terrorist financing, the customs officers themselves have also powers to stop or restrain the currency on the basis of the provisions in the Customs Act, 1962 (ss.2(22), 110, 111(d), and 113(d)). A suspicion of

28

An authorised person (AP) means an authorised dealer, money changer, off-shore banking unit or any other person for the time being authorised under section 10(1) of the Foreign Exchange Management Act (FEMA) to deal in foreign exchange or foreign securities.

terrorist financing may be drawn on the basis of the lists of designated terrorist entities, which are circulated by the MEA to the customs administration and included by the latter in its database. In addition, as indicated above (see Section 2.3), section 25 of the Unlawful Activities (Prevention) Act (UAPA) provides for seizure of property which represents proceeds of terrorism. So far, no such instances with regard to terrorist financing have been reported, although customs officers may also alert the State Police to initiate their own enquiries under the UAPA.

False declaration/ disclosure

357. Where there is a false declaration or disclosure regarding cross border transportation of cash and BNI, the cash and the BNI are liable for confiscation under sections 111(d) or 113(d) of the Customs Act. Section 110 of the Customs Act provides that if the customs officer has reason to believe that goods are liable to confiscation, they may be seized. The term 'goods' is defined in the Customs Act (s.2(22)) and includes (a) vessels, aircrafts and vehicles; (b) stores; (c) baggage; (d) currency and negotiable instruments; and (e) any other kind of movable property. Further, section 110 of the Customs Act provides that if the proper officer has reason to believe that any goods are liable to confiscation under the Act, he may seize such goods. Based on these provisions Indian authorities are able to stop or restrain currency and BNI.

358. The provisions in India with respect to the seizure, attachment and forfeiture of proceeds of crime or funds for terrorist activities also apply to the cross-border movements of currency or BNI. When there is a suspicion that the funds may be related to money laundering or terrorist financing, the various provisions described in Section 2.3 of this report apply.

Information collected

359. The customs authorities forward Currency Declaration Forms (CDFs) collected at both the Indian airports and land borders to the Central Economic Intelligence Bureau (CEIB) in a prescribed format which includes information regarding the reported person (name, passport number, nationality, address, etc.), the currency declared (name of the currency, details of the currency notes, details of other instruments), and the currency seized (names of the currency, details of currency and details of other instruments).

360. After the restructuring of the CDF Data management system in 2009, all the data regarding CDFs which are received by the CEIB are shared with the FIU-IND and other relevant agencies. The CEIB, after entering the details of CDFs in its database, carries out analysis on the basis of several parameters which include frequency of visits, amount of the foreign currency declared and the related inputs available within the CEIB. The results are provided to the FIU and the other concerned agencies including Directorate of Enforcement (e.g. the CEIB has forwarded analysis of few CDFs wherein the passengers had filed CDFs on more than one occasion or where the nationality of the passengers was considered as high risk). The FIU has integrated the CDF database in its analytical search engine.

Sanctions

361. Sections 112 and 114 of the Customs Act allow imposing a penalty on a person who, in relation to any goods, including currency and BNI, does or omits to do any act which would render such goods liable to confiscation under section 111 (improper import) and section 113 (improper export) of the Act. The Indian authorities state that these provisions are applicable to persons who make a false declaration or fail to make a declaration, as required by the FEMA. In addition, the Customs Act also provides for imprisonment, or a fine, or both, of persons who make, sign, or use false declarations (Customs Act ss.132 and 135). Section 140 foresees that if the contravention is by a company, then the directors are also liable for a penalty. This implies that the penal provisions in the Customs Act apply to both natural and legal persons; however, there is no definition of person in the Customs Act and consequently, the provisions of the General Clauses Act apply.

362. Section 13 of the FEMA foresees a monetary penalty for any person who contravenes any rule, regulation, notification, direction or order issued in exercise of the powers under this Act, which includes the declaration obligation in the Regulations. Based on section 42 of the FEMA, not only companies but also their directors are liable for a monetary penalty if the contravention is made by a company.

363. A person who is carrying out a physical cross-border transportation of currency or BNI that are related to money laundering commits the ML offence and is punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to a fine which may extend to INR 500 000 (USD 10 000) (PMLA s.4). In such cases, the attachment, confiscation and forfeiture provisions discussed in Section 2.3 above would apply.

364. A person who is carrying out a physical cross-border transportation of currency or BNI that are related to terrorist financing is considered to be holding terrorist funds, which is punishable by a maximum term of life imprisonment, and shall also be liable to a fine (UAPA s.21). If the person carries the currency or the BNI with the intention of furthering the activity of a terrorist organisation, then such person is punishable with imprisonment for a term not exceeding 14 years, or with a fine, or with both (UAPA s.40). The provisions of the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order and the UAPA relating to the freezing, seizing and attachment of property related to terrorist financing (as discussed in Section 2.4) apply to currency or BNI that are transported across the border and are related to terrorist financing.

Domestic and international co-operation and co-ordination

Domestic co-operation

365. An Air Port Co-ordination Committee (APCC) meets for the purpose of co-ordination among customs, immigration and other related authorities, and for sharing and dissemination of information in relation to important cases of economic offences. The Committee is mandated to hold quarterly meetings during which information collected and modus operandi are discussed and shared, including cross-border movements of cash or BNI.

International co-ordination

366. India has been a member of the World Customs Organisation (WCO) since 1971 and has participated in developments in the fields of classifications, valuation, customs procedures and enforcement. In order to assist its members to improve the effectiveness of their enforcement efforts, the WCO has established Regional Intelligence Liaison Offices (RILOs) and India is a member of the Regional Intelligence Liaison Office in the Asia-Pacific region (RILO-AP). India has been actively participating in the Central Contact Point programme of the RILO-AP and has shared useful information through this RILO. It also receives the reports and publications issued by the RILO-AP. India has also actively participated in customs co-operation programmes such as SKYHOLE PATCHING and PROJECT FAIRPLAY co-ordinated by different RILOs. In 2009, Indian Customs has participated in Operation ATLAS which was undertaken by 80 Member countries of the WCO, the largest multilateral operation in history targeting cash smugglers which took place from 26 to 30 October 2009.

367. The Customs Enforcement Network (CEN) is an internet based information system for data exchange and communication between and among customs services which has been set up to facilitate co-operation regarding dissemination of information and intelligence and enforcement. CEN has three main elements: (a) a database of seizures and offences; (b) a website; and (c) a communication system (CENCOMM). The RILOs utilise the database of seizures and offences which includes analytical capacity regarding modus operandi, trends, concealment methods, routes, etc., to prepare various useful reports and other documents. In India, the DRI is in charge of compiling, analysing and further disseminating of information regarding customs offences, including data related to cross border transportation of currency

and BNI, detected across the country. It inputs offence data pertaining to significant cases in CEN, including those pertaining to seizures of currency, gold and precious stones.

368. The Indian customs has signed 16 Customs Mutual Assistance Agreements (CMAA), covering a total of 46 countries, including the United States; the United Kingdom; France; Russia and China. These agreements establish the formal mechanism for exchange and sharing of intelligence and information between the CBEC and the customs authorities of the various countries. The agreements foresee, among other things, the instances in which the customs authorities can share intelligence and information on terrorist activity, trade fraud, narcotics trafficking, smuggling of weapons of mass destruction, and container security violations.

369. In the absence of a formal CMAA, co-operation and assistance is extended by Indian customs authorities on the basis of reciprocity. A Customs Overseas Intelligence Network (COIN) has been set up to facilitate the exchange of information with customs administrations of other countries (within the framework of bilateral co-operation agreements or under the Nairobi Convention) as well as to assist the Indian customs authorities with intelligence gathering and investigation relating to customs offences. At present, eight COIN units are located in London; Dubai; Hong Kong, China; Brussels; Moscow; New York; Singapore; Kathmandu and Birganj and it is intended to further expand this network in the future. Intelligence shared through COIN with overseas enforcement agencies has resulted in seizures of offending goods, including drugs and Fake Indian Currency Notes (FICN) within and outside India.

Safeguards for protecting information

370. The proper use of the information/data that is obtained by the customs authorities through the system of reporting of cross border transactions is safeguarded by section 136(3) of the Customs Act. In addition, the bilateral and regional co-operation agreements also contain a specific clause on the subject of "Information exchange and confidentiality". The bilateral/regional agreements generally also provide for exemption from providing assistance in case such assistance may prejudice any legitimate commercial or professional interest of the person concerned (Article 16 of the agreement with South Africa and Article 16 of the agreement with the EU).

371. Section 5 of the Official Secrets Act, as discussed above in relation to other government officials, provides for punishment for a person who has in his possession any information which he has obtained or to which he has access owing to the position he holds under the Government and wilfully communicates the information to any person other than the person to whom he is authorised to communicate it or fails to take reasonable care of the information.

Gold and Precious Metals/Stones

372. The cross border movement of gold is regulated in India with gold dealers being required to register (and thereby become a Nominated Agency) with the Reserve Bank of India (RBI) in order to transact payments for gold purchases. Gold retailers must transact through a nominated agency. Any unusual cross border movement of gold, precious metals or precious stones that is discovered by Customs is notified to the appropriate agencies, including via the Customs Enforcement Network (CEN), an internet based information system for data exchange and communication between and among customs services which has been set up to facilitate co-operation regarding dissemination of information and intelligence and enforcement.

Additional elements

373. India has implemented some major parts of the measures in the Best Practices Paper for SR.IX, including the threshold declaration obligation for foreign currency and BNI by incoming passengers. In addition, X-ray baggage inspection and screens and X-rays of bodies of suspected persons take place.

374. As indicated above, the CEIB receives the currency declarations forms from the customs regional offices and the details contained in it are maintained in a computerised database and shared with the FIU and other relevant agencies.

Recommendation 30 - Structure, funding, staffing and resources (customs authorities)

375. The Indian Customs has in excess of 72 000 staff. It draws its officers from the IRS and recruits other executive staff through the Public Service Commissions. The customs administration functions under the administrative control of the CBEC, but enjoys operational independence and autonomy. In addition, customs officers are located at 'foreign' postal service agencies, these being post offices in India that deal only with foreign postal services, and actively investigate any matters of interest through the foreign postal system, including the sending of currency via postal services.

376. Adherence to the Government of India Conduct Rules by the customs officers is ensured through a system of checks and balances in the use of discretionary power, discreet surveillance, and awareness raising campaigns. As public servants, staff of the Indian Customs service is also subject to procedures of the CVC.

377. Training in the form of induction courses and refresher courses is provided at the National Academy of Customs Excise and Narcotics at Faridabad (NACEN), which is the training institute for the Central Excise, Customs and Narcotics Department of India. These training initiatives also include training on combating money laundering and terrorist financing. NACEN has also been recognised as the Regional Resource Centre of the WCO. NACEN is regularly providing AML training to all grades of customs officers at its headquarters and at its 9 regional centres. These training modules have the obligations under the FEMA as one of their components.

Recommendation 32 – Statistics

378. The total number of Currency Declaration Forms (CDFs) collected at international airports in India for cross border currency transportation is set out in the table below:

| 2005-2006 | 2006-2007 | 2007-2008 | 2008-2009 | April 2009 - October 2009 | Total |
|-----------|-----------|-----------|-----------|---------------------------|---------------|
| 8 310 | 8 592 | 10 064 | 9 573 | 4 960 | 41 499 |

The Indian authorities are not in a position to provide details regarding the number of CDFs collected at Land Customs Stations.

379. Section 6 of the FEMA empowers the RBI to prohibit, restrict, or regulate, inter alia, the export, import, or holding of currency or currency notes. Further, the Government has empowered, by application of the Regulations, customs officers to exercise the powers and discharge the duties of the Director of Enforcement in so far as they relate to restrictions/prohibitions imposed by the RBI on the import and export of currency. Therefore, violations of the FEMA in this regard are adjudicated by the customs authorities, and the fines imposed for non-declaration or misdeclaration of currency are imposed by the customs authorities in respect of violation of both the FEMA and the Customs Act, which prohibits the import or export of goods in violation of any prohibition placed by any other law in force. The statistics in this regard are as follows:

Statistics: Fines imposed under FEMA and Customs Act in cases of non declaration or misdeclaration of currency

| Financial year | No. of cases involving non declaration or misdeclaration of currency | Value of foreign currency in INR | Redemption fine imposed in INR | Personal Penalty imposed in INR |
|----------------|--|----------------------------------|--------------------------------|---------------------------------|
| 2006-2007 | 68 | 829 000 | 101 000 | 146 000 |
| 2007-2008 | 70 | 1 187 000 | 279 000 | 190 000 |
| 2008-2009 | 52 | 997 000 | 110 000 | 501 000 |

Statistics: Seizures of Indian and Foreign Currency

| | 2007-2008 | | 2008-2009 | |
|------------------|--------------|--------------|--------------|--------------|
| | No. of cases | Value in INR | No. of cases | Value in INR |
| Indian currency | 194 | 16 453 500 | 255 | 42 976 570 |
| Foreign currency | 552 | 111 578 950 | 606 | 76 840 990 |

These cases relate to smuggling of currency and no direct linkages to FT have been identified.

Implementation and effectiveness

380. The Arrival Card for Passengers, which is the process used to inform incoming passengers of the currency declaration requirements, is not clear on its face in relation to the legal requirements on this issue and this may in turn impact on the effectiveness of the cross border currency transportation procedure. For example, the fields on the Arrival Card that are required to be completed by the passengers do not mention the legal obligation concerning the declaration of the carriage of currency and there is no discreet place for the passengers to declare on this form whether they are or are not carrying an amount in excess of the regulated limits (e.g. the currency declaration form to which the information on the reverse of the Arrival card refers is not attached to the Customs Declaration Form nor is it indicated where it can be obtained).

381. The effectiveness concern expressed above seems to be confirmed by the low number of cash declarations made at international airports, and the absence of information relating to the movement of currency across land border stations, taking into account the size and the cash based nature of India's economy and the volume of international travellers in India. In addition, the number of false declarations and the corresponding volume of cash seizures are extremely limited. The figures regarding the seizure of Indian and foreign currency involved very few cases where there was a suspicion of money laundering, while, as indicated above, there were no such cases based on a suspicion of terrorist financing.

382. On the reverse of the Arrival Card there is information relating to the obligations on passengers, and this includes reference, in paragraph 4 on Information Regarding Customs, that "... passengers should declare foreign currency in the currency declaration form, if currency notes, bank notes, or travellers cheques are in excess of [the prescribed amount]". On the basis of the advice given on the reverse side of the form, passengers may not appreciate the strict legal obligation to disclose the carriage of currency through the border and the legal consequences of not respecting this obligation.

383. A further issue with the Arrival Card for passengers concerns the limited range of 'currency' types referred to in paragraph 4 of the reverse side of this form (*i.e.* refers to currency notes, bank notes and traveller's cheques). Based on this advice passengers are unlikely to appreciate the legal obligation to disclose the wider range of BNI covered by the Regulations. In addition, the system for currency

declaration forms seems to be applied only at international airports, with no apparent reporting from land border posts.

2.7.2 Recommendations and Comments

384. As noted, India's cross border declaration and disclosure regime established under the Foreign Exchange Management Act (FEMA) was designed for the purpose of facilitating external trade and payments, and for promoting the orderly development and maintenance of the foreign exchange market in India, and part of this system includes regulating the cross border movement of currency and BNI's. However, in addition to concerns relating to the effective implementation of this system for AML/CFT purposes, there are technical deficiencies in relation to which India should consider amending its legislation.

385. The declaration system is used only in relation to the importation of currency and is not used for the export of currency from India, hence there is no information on the extent to which Indian or foreign currency is being moved out of India. In terms of currency declaration forms (CDFs) for importation of currency, these seem only be used at international airports. Although the Indian authorities inform the assessment team that the declaration obligation equally applies to movement of currency via land, no statistics regarding such movements of currency are available what gives an indication of an ineffective implementation of the declaration obligation at land borders. Given the very large number of people moving across the Indian borders, the cash based nature of its economy, the number of CDFs declared, and the number of false declarations detected, the number of cash seizures on an annual basis are very low. This points to an issue regarding the effectiveness of the implementation of both the declaration scheme for importing and the disclosure regime for export of currency and BNI's. The arrival card for incoming passengers provides the prompt for CDFs, however the arrival card itself is deficient in terms of guidance – with no field for acknowledging the carriage of currency above the threshold and an inadequate guidance note as to the strict legal nature of the requirement to disclose this information.

386. The Indian authorities should undertake an in-depth analysis and envisage taking the necessary actions based on the deficiencies identified above.

387. The Indian authorities should introduce targeted actions for the detection of smuggling of currency and BNI via containerised cargo or mail.

388. India should take action to address the deficiencies identified in relation to the implementation of the FATF Recommendations, as identified in Sections 2.3 and 2.4 of this report that have a negative impact on Special Recommendation IX.

2.7.3 Compliance with Special Recommendation IX

| | Rating | Summary of factors relevant to s.2.7 underlying overall rating |
|-------|--------|---|
| SR.IX | PC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns based on the low number of currency declarations, the detected false declarations, and the cash seizures, including seizures of unaccompanied cash or BNIs. • The Cross border declaration/disclosure systems appear to be applied only to currency and BNI via airports, with no information on movements of currency and BNI via land borders or unaccompanied movement of currency through postal and cargo systems. • The shortcomings identified with regard to the attachment, confiscation and forfeiture provisions discussed in Section 2.3 and to the freezing, seizing and attachment of property related to terrorist financing (as discussed in Section 2.4) have a negative impact on Special Recommendation IX. |

3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS

Preamble: Scope issue

389. The provisions of Chapter IV of the PMLA, imposing AML obligations on the financial sector, applied initially to banking companies, financial institutions and intermediaries. Through cross-reference to the definitions in the RBI, SEBI and Banking Regulation Acts, these terms are defined under section 2 of the PMLA to embrace all entities that are regulated for prudential purposes by the RBI and the SEBI, but also capture insurance companies within the definition of “non-bank financial companies”. However, after legislation was enacted in 1999 to create the IRDA with a mandate to regulate the insurance sector, the RBI formally exempted the insurance sector from its supervisory oversight in order to avoid dual regulation (although the relevant section within the RBI Act was never amended).

390. Since the amendments to the PMLA were enacted on 6 March 2009, the term “financial institution” has been expanded to include Authorised Persons as defined in section 2(c) of the FEMA, and payment system operators. An Authorised Person (AP) means an authorised dealer, money changer, off-shore banking unit or any other person for the time being authorised under section 10(1) to deal in foreign exchange or foreign securities. This includes India Post, which is authorised by the RBI with respect to its foreign exchange operations²⁹. A payment system operator is defined under the PMLA to include a person who enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service. A payment system includes credit, debit, smart card and money transfer operations.

391. Based on the definitions in section 2 of the PMLA, the following entities are now covered by the preventive provisions in chapter IV of the PMLA. Those categories marked with an asterisk were brought into the regime by the March 2009 amendments to the PMLA, which came into effect on 1 June 2009.

| Banking Companies | Financial Institutions | Intermediaries |
|--|---|---|
| <ul style="list-style-type: none"> • Public sector banks • Private Indian banks • Private foreign banks • Co-operative banks • Regional rural banks | <ul style="list-style-type: none"> • Insurance companies • Hire purchase companies • Chit fund companies • Housing finance institutions • Non-banking financial companies • Including casinos* • Payment system operators* • Authorised money changers* | <ul style="list-style-type: none"> • Stock brokers and Sub-brokers • Share transfer agents • Bankers to an issue • Trustees to trust deed • Registrars to issue • Merchant bankers • Underwriters • Portfolio managers • Investment advisers • Depositories and Depository Participants • Custodian of securities • Foreign institutional investors • Credit rating agencies • Venture capital funds • Collective investment schemes, including mutual funds |

* Brought under the PMLA with effect of 1st June 2009

²⁹ India Post provides a range of financial services, including savings and deposit accounts, life insurance, mutual funds and money remittance within India (through the issuance of money orders). The India Post website states that it is the largest retail bank in the country operating 220 million savings accounts from 150 000 branches. These deposit-taking activities are not covered by the primary banking or financial services laws, but are governed by the Government Savings Bank Act. However, since India Post is a “financial institution” for the purposes of the PMLA (by reason of being an Authorised Person with respect to its foreign exchange operations), all its financial services activities are subject to the provisions of the PMLA. Despite this, India Post is not supervised by the mainstream financial services regulators (except for its foreign exchange business), and, this role falls, instead, to the Ministry of Finance audit department.

392. This list embraces all the financial activities required to be covered under the FATF standards, with the exception of commodities futures brokers. This omission from the scope of the PMLA is of limited materiality.

393. While insurance intermediaries and agents are not specifically referenced in the definitions in the PMLA, these activities are considered to be captured under the obligations imposed on the insurance companies themselves. Insurance intermediaries in India are tied agents working solely for one insurance company, and are deemed to be integrated into the insurer for systems and controls purposes. The IRDA instructions (see below) impose specific obligations on the insurers to ensure that their agents comply with the same obligations as those imposed directly on the insurers.

Preamble: Law, regulation and other enforceable means

The PMLA

394. Chapter IV of the PMLA, which sets the obligations for banking companies, financial institutions and intermediaries, is very brief, containing only four short sections, two of which (on record-keeping and reporting to the FIU) provide for further elaboration through measures that may be prescribed at a later date. Such measures are introduced under section 73 of the PMLA, which provides the Central Government with rule-making powers.

The PML Rules

395. Most of the PML Rules became effective on 1 July 2005, when the PMLA itself came into force. However, additional Rules were notified on 12 November 2009 to expand the scope of the regulatory agencies that are able to exercise powers under the Rules (beyond the core financial sector regulators), and to strengthen the preventive measures. A further, short amendment was made on 12 February 2010, the final day for it to be taken into consideration within this report under the “two month rule”. The structure of these Rules is such that they qualify for consideration as “law or regulation” and, therefore, would be a suitable medium for the introduction of the core (asterisked) elements of Recommendations 5, 10 and 13. This is based on the facts that, under section 74 of the PMLA, the Rules must be laid before both houses of parliament for a total period of thirty days to permit parliament either to modify or annul individual Rules.

396. In issuing Rules under the PMLA, the authorities have adopted the practice of promulgating a series of individual “Notifications”, each of which addresses a particular topic and includes its own short title, date of commencement and set of definitions. Notification 9 of 1 July 2005 contains 11 sub-rules, which are called the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005. These sub-rules only stipulate general procedural requirements, and do not extend to addressing a wide range of key issues. Sub-rules 5(3) and 7(4), as amended through to November 2009, provide that the appropriate regulator may issue instructions in relation to the maintenance of records and provision of information to the competent authorities. A further amendment to the Rules was notified on 12 November 2009, which expanded the circumstances in which the regulators could issue instructions under the Rules, to include the ability to “prescribe enhanced measures to verify the client’s identity taking into consideration the type of client, business relationship or nature and value of transactions”. Notification 9 and its amendments are simply referred to as the PML Rules in this section of the report.

The Circulars issued by the regulatory authorities

397. Each of the regulators issues “circulars” to the sectors for which they are responsible, specifying requirements in relation not only to the matters specifically delegated to the RBI, SEBI and IRDA under

the PML Rules, but also more broadly. The regulators' authority to issue specific instructions is provided under Rule 5 and 7 of the PML Rules and powers to issue more general instructions are contained in each of the regulators' governing legislation. Under the original July 2005 Rules, only the RBI and SEBI were recognised as competent authorities to issue instructions, but the IRDA was subsequently incorporated through a notification issued in December 2005. The range of competent authorities was further expanded by the notification of 12 November 2009, which introduced the definition of a "regulator" as a person, authority or government which is vested with the power to license, authorise, register, regulate or supervise the activity of banking companies, financial institutions or intermediaries. This does away with the need to specify individual agencies.

398. For the most part, the language of the circulars is mandatory in nature ("shall", "must" or "should") and the financial institutions confirmed that they consider that the circulars must be implemented in full. Any contravention or non-compliance with the instructions issued by the regulators is stated to be liable to attract penalties under specific provisions of the relevant Acts (e.g. breaches of the Master Circular issued to the banks may be sanctioned under section 47A of the Banking Regulation Act); and the authorities have provided data to show the range of sanctions that have been applied for failure to implement the specific requirements in the circulars (see discussion under Recommendations 5 and 17), although there are concerns that the sanctions themselves may not always be effective, proportionate and dissuasive. However, this relates more to the effectiveness of implementation, rather than the legal status of the circulars. Therefore, insofar as the language of the circulars is mandatory, they are considered to be "other enforceable means" (OEM).

399. In considering the guidance issued by the various regulators, it has to be noted that there is no correlation between the definitions of "financial institution" used, respectively, in the PMLA and regulatory laws administered by the RBI. The PMLA now provides a definition that goes substantially beyond the scope of the term used by the RBI when issuing instructions to entities under its own legislative authority; and this variation has been extenuated further by the inclusion, in the March 2009 amendment to the PMLA, of payment services operators, authorised money changers and casinos within the definition of financial institutions for the purposes of that Act. The situation is further complicated by the fact that, as a result of the evolution of the RBI's responsibilities, different institutions are supervised by different departments within the RBI, all of which issue their own circulars. The position with respect to the SEBI and IRDA is much simpler. The following table seeks to show how responsibility is allocated for the range of institutions, as defined in the PMLA.

| PMLA Definition | Class of entities | Regulatory Department/Institution |
|--|---|---|
| Section 2(e) of the PMLA - "banking company" means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949) applies and includes any bank or banking institution referred to in section 51 of that Act" | Scheduled Commercial Banks | RBI Department of Banking Operations and Development |
| | Urban Co-operative Banks | RBI Urban Banks Department |
| | Regional Rural Banks/State Co-operative Banks/District Central Co-operative Banks | RBI Rural Planning and Credit Department |
| Section 2(l) of the PMLA - "financial institution" means a financial institution as defined in clause (c) of section 45-l of the Reserve Bank of India Act, 1934 (2 of 1934) and includes a chit fund company, a co-operative bank, a housing finance institution, an Authorised Person, a payment system operator and a non-banking financial company" | Non-Banking Financial companies <i>(includes casinos)</i> | RBI Department of Non-Banking Supervision <i>(Government of Goa)</i> |
| | All-India Financial institutions (e.g. NHB, NABARD, EXIM Bank and SIDBI) | RBI Department of Banking Operations and Development |
| | Housing Finance institutions | National Housing Bank |
| | Securities intermediaries | SEBI |
| | Insurance companies | IRDA |
| | Authorised Person Money Changers (includes money changers and Indian agents of Money Transfer Service Providers, and India Post's FX operations) | RBI Foreign Exchange Department |
| | India Post (non-FX financial services) | Ministry of Finance |
| | Payment system operators (e.g. VISA, MasterCard etc.) | RBI Department of Payment and Settlement Systems |
| | Chit funds ³⁰ | State Governments |

400. The relevant circulars issued by the various regulators and considered to be enforceable (under either the PML Rules or the regulators' own statutory powers) are referenced below.

401. ***Institutions supervised by the RBI:*** The RBI has issued circulars under section 35A of the Banking Regulation Act for banking companies and other financial institutions; under section 45K and 45L of the RBI Act for non-bank financial companies; and under sections 10(4) and 11(1) of the Foreign Exchange Management Act (FEMA) for Authorised Persons in Foreign Exchange. The various regulatory

³⁰ With effect from 29 August 2009 chit funds were prohibited from accepting deposits from other than shareholders.

departments have issued different circulars, which tend to be similar, but not identical, in content, even allowing for necessary variations to reflect the different types of business being undertaken.

- a. *RBI Guidance for scheduled commercial banks and all financial institutions*: On 1 July 2009, the RBI issued a Master Circular on Know Your Customer norms/Anti-Money Laundering standards/Combating of Financing of Terrorism/Obligations of banks under the PMLA. A supplement was issued in 11 September 2009. The Master Circular consolidates various instructions that were issued by the RBI up to 30 June 2009. This guidance also applies to Offshore Banking Units (OBUs) in the Special Economic Zones (SEZs) based on an instruction dated 12 November 2002, which requires OBUs to follow AML requirements issued for commercial banks and all financial institutions. These units operate effectively as a division within the domestic bank.
- b. *RBI Guidance for Urban Co-operative banks (UCBs)*: Between December 2004 and November 2009, the RBI issued ten circulars to UCBs on KYC/AML/CFT Guidelines, wire transfers, and obligations under the PMLA. Some of the guidance documents have updated others, but no consolidated version has been issued for this sector.
- c. *RBI Guidance for State/District Central Co-operative Banks (StCB/DCCBs)*: Between February 2005 and June 2008, the RBI issued five relevant circulars to StCB/DCCBs, but no consolidated version has been issued. While the RBI has the authority to issue such circulars to this sector, responsibility for ensuring compliance is vested in the National Bank for Agriculture and Rural Development (NABARD).
- d. *RBI Guidance for Regional Rural Banks (RRBs)*: Between February 2005 and June 2008, the RBI issued five circulars to RRBs, but no consolidated version has been issued for this sector. The same distinction, as noted above, between the roles of the RBI and the NABARD applies for this sector.
- e. *RBI Guidance for Non-Banking Financial Companies (NBFCs)*: Between February 2005 and August 2008, the RBI issued six circulars to NBFCs. A Master Circular was issued on 1 July 2009 consolidating all the previous circulars and attaching a version of the Master Circular issued to the commercial banks. The introduction specifies that the provisions of the banking circular are applicable equally to the NBFCs, insofar as they are relevant to the business being undertaken by individual institutions. An addendum to the Master Circular was issued on 13 November 2009 to mirror certain provisions applied to the banking sector on 11 September.
- f. *RBI Guidance for Authorised Money Changers (AMCs)*: Between December 2005 and March 2009, the RBI issued four wide-ranging circulars to AMCs, which included elements of AML/CFT requirements, but since AMCs were not captured under the PMLA until the introduction of the March 2009 amendment, the circulars were issued solely under section 10(4) and section 11(1) of the FEMA. The limited AML/CFT provisions of the latest general circular (issued on 9 March 2009) were replaced by a specific AML/CFT circular issued on 27 November 2009. This circular (now issued under both the FEMA and the PML Rules) applies to all Authorised Persons under section 2 of the FEMA, and states that agents and franchisees are required to adhere to the same AML/CFT standards as the primary company.
- g. *RBI Guidance for Indian Agents under Money Transfer Schemes*: The RBI issued this guidance on 27 November 2009. It relates to those institutions that are authorised to act as the local agent for funds transferred from abroad by “reputed money transfer companies”. The agent does not undertake the exchange transaction itself (this takes place in the overseas jurisdiction), but acts as the remitting agent for the proceeds. The provisions of the circular broadly reflect those of the instruction issued to AMCs on the same date, insofar as they are

relevant to the agents' business. As is the case with the AMCs, this circular is issued under the relevant provisions of both the FEMA and the PMLA.

- h. *RBI Guidance for Payment Systems Operators*: This guidance was issued on 22 December 2009 (*i.e.* after the on-site visit). It addresses only cash and suspicious transaction reporting requirements.

402. The RBI has not yet issued specific AML/CFT guidance for money remitters, except insofar as these activities are undertaken by banks that are covered by the RBI circulars described above. While the Payment and Settlement Systems Act (PSSA) envisages the possibility for the RBI to authorise domestic money remitters (as distinct from those entities authorised under the FEMA to act as the Indian agent for cross-border transfers), no such licences have yet been issued, and this activity (on a lawful basis) is currently reserved for the banks and India Post. Since February 2009, authorisations have been issued under the PSSA to 29 other entities engaged in a range of payments system activities (central clearing, card payments, ATM services, pre-paid instruments). As a specific condition of their authorisation, all such entities are required to follow the bank circulars, insofar as the provisions are relevant to their business.

403. The circulars issued by the RBI to the various categories of financial and non-financial institutions (with the exception of those issued to the authorised money changers) are broadly similar in scope and content, although there are variations in order to take into account the differences in the nature of the underlying business. Consequently, the following analysis of the CDD obligations will address all the institutions supervised by the RBI as a single category (with the exception of the AMCs), with reference being made primarily to the Master Circular issued to the scheduled commercial banks and financial institutions. Where there are any material differences between the different sets of instructions, these are highlighted.

404. The position with respect to India Post is complex. Following its inclusion under the PMLA in June 2009, India Post became subject to the RBI circular issued to Authorised Persons with respect to its foreign exchange operations. As regards its deposit-taking activities, the Department of Posts within the Ministry of Communications and IT issued an office memorandum in January 2010 outlining some basic AML/CFT requirements in respect of STRs, record-keeping and the role of the compliance officer. This was subsequently replaced by new office memoranda issued on 12 and 23 April by the Ministry of Finance's Department of Economic Affairs. The legal status of these documents is unclear, but in any event, for the purposes of this evaluation, it has not been possible to determine the extent of implementation of these instructions, given the very recent date of their promulgation.

405. ***Intermediaries supervised by SEBI***: The SEBI issued a Master Circular to all intermediaries on 19 December 2008 under Section 11(1) of the Securities and Exchange Board of India Act (SEBI Act) and the PML Rules (in general). A set of amendments was issued on 1 September 2009, following a review undertaken ahead of the FATF mutual evaluation, and a revised version of the Master Circular (with further amendments) was issued on 12 February 2010. Non-compliance with these circulars is liable to attract penalties under the relevant provisions of the SEBI Act and the accompanying Regulations. Regulation 17 read with Chapter IV of the SEBI (Intermediaries) Regulations, 2008 provide for inspection and disciplinary proceedings, and Regulation 17(2) indicates that one of the purposes of such inspection is to ascertain whether the registered intermediaries comply with the provisions of the securities laws and the relevant directions or circulars. Chapter V of these Regulations contains specific provisions relating to actions the SEBI may take in cases of non-compliance. In addition, since day-to-day supervision of the intermediaries is undertaken by the exchanges and the depositories for their respective intermediaries, they issue circulars that mirror those of the SEBI, so that they have a direct basis for exercising their own disciplinary powers.

406. **Insurance companies:** The IRDA has been empowered by the amendments to the PML Rules, introduced by Notification 13 of December 2005, to issue relevant instructions to the entities that it regulates. On this basis, the IRDA has issued ‘AML guidelines to insurers’ under section 34 of the Insurance Act, 1938. On 24 November 2008, the IRDA issued a Master Circular (updated to 31 October, 2008), which consolidates all its previous AML/CFT circulars. A set of amendments was subsequently issued on 24 August 2009, following a review of the circular in advance of the FATF mutual evaluation, and further additions were introduced on 3 February 2010. Under section 102 of the Insurance Act, the IRDA has the authority to levy fines for non-compliance with directions issued under section 34, while section 14 of the IRDA Act empowers it to withdraw, suspend or cancel the registration of an insurance company. The Master Circular applies to insurance companies, but not directly to their agents and other intermediaries. However, in India, insurance agents are “tied” agents, who are permitted to work for one insurer only, and section 3.1.11 of the circular imposes the obligation upon the insurer to establish internal regulations governing the agents’ operations and to have procedures to enforce them. In practice, therefore, the agents are acting as an integral part of the individual insurers, and the insurers can be sanctioned for failures by the agents to implement procedures in line with the Master Circular.

Industry guidance

407. In July 2009, the Indian Banks’ Association (IBA) issued a set of AML/CFT guidance notes to its members. While these notes are a helpful illustration of the PMLA and regulatory requirements, and, to some extent, go further than the regulatory requirements, it is specifically stated that they are voluntary in nature, and that failure to comply with the guidelines does not mean that a bank has breached the PML Rules or the guidelines issued by the RBI. Therefore, the IBA guidance is not given further consideration in this report.

408. In other sectors, the Life Insurance Council has considered specific issues on a case-by-case basis, and has provided *ad hoc* guidance to its members, and the Association of Mutual Fund in India issues regular guidance to the industry on the CDD and STR obligations.

3.1 Risk of money laundering or terrorist financing

409. The authorities have not undertaken a comprehensive risk assessment of all the financial institutions operating in India, but some assessments have been completed for individual sectors. Various inter-ministerial committees and groups, under the umbrella of the Ministries of Finance and Home Affairs, are in place to review the threats, vulnerabilities and risks in different parts of the financial sector. These reviews have not resulted in any decisions to exclude specific institutions or types of activity from the AML/CFT regime on the basis that they pose a low or negligible risk for ML/FT purposes. Therefore, the exclusion of the commodities futures brokers from the PMLA is not based on a risk assessment.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis

Recommendation 5

410. The November 2009 amendment to sub-rule 7(ii) of Rule 9 of the PML Rules introduced a requirement that all covered institutions must formulate and implement a Client Identification Programme incorporating the requirements laid down in the Rules and any instructions issued by the regulatory authorities. For the most part, this simply codified the high-level requirement that already existed in the Master Circulars published by the individual regulators.

Anonymous accounts

411. Section 12(1)(c) of the PMLA imposes an obligation on all covered institutions to verify and maintain records of the identity of all its clients, in such a manner as may be prescribed. Rule 9 of the PML Rules requires every such institution, at the time of opening an account or executing any transaction, to verify the identity, address, nature of business and financial status of the client. The Rule then stipulates the types of identification documentation that are relevant for different categories of customer (personal, corporate, partnership, trust, unincorporated association). These provisions would, in principle, be sufficient to prohibit the opening of anonymous accounts, but the amendment to the PML Rules published on 12 November 2009 states specifically that financial institutions shall not keep any anonymous accounts or accounts in fictitious names. The RBI, SEBI and IRDA circulars provide additional instructions that no account is to be opened in anonymous or fictitious/benami³¹ name(s).

When CDD is required***All institutions covered by PMLA***

412. Rule 9 of the original 2005 PML Rules required institutions, at the time of opening an account or executing any transaction, to verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status. The term transaction is defined in Rule 2(h) to include a “deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means”. There was no minimum threshold, in terms of value, for when CDD must be undertaken on an occasional transaction, and so all transactions undertaken by all covered institutions were caught by the requirement. Following the 2009 amendment to the PMLA to expand the range of institutions captured by its provisions, the revised PML Rules of November 2009 introduced a distinction between account-based relationships and occasional transactions. While the basic principles applied to account-based relationships remained unchanged, a threshold of INR 50 000 (USD 1 000) was introduced for occasional transactions (including multiple transactions that appear to be linked), except in relation to “international money transfers”, for which there remains no threshold.

413. The CDD provisions, at the level of law and regulation, do not refer to situations where there is a suspicion of money laundering or terrorist financing or where an institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Institutions supervised by the RBI (except AMCs)

414. Section 2.4(a) of the RBI Master Circular repeats the core elements of the Rules, but extends the obligation to undertake CDD to circumstances in which a bank has doubts about the authenticity, veracity or adequacy of the previously obtained identification data. However the circular (which does not constitute “law or regulation”) is silent on the need to revisit the CDD measures when there are suspicions of money laundering or terrorist financing.

Securities sector

415. Section 5.5 of the SEBI Master Circular also includes the provision that the intermediaries’ CDD policies must include procedures for undertaking additional CDD when there are doubts about the veracity or adequacy of previously obtained information on the customer. As with the RBI circular, there is no explicit obligation to revisit the CDD when there are suspicions of money laundering or terrorist financing.

³¹ Benami transactions are transactions conducted in the name of a person who does not pay any consideration for the underlying asset, but merely lends his name while the real title remains vested in the true owner. The *Benami Transactions (Prohibition) Act, 1988* sought to prohibit such transactions (essentially by removing the ability of both parties to claim title to the asset).

Insurance sector

416. The IRDA Master Circular adds nothing to the Rules in respect of the circumstances in which CDD should be undertaken.

Authorised Money Changers

417. The November 2009 circular to Authorised Persons requires that institutions establish a policy, approved by the board, which “should clearly spell out the Customer Identification Procedure to be carried out at different stages, *i.e.* while establishing a business relationship; carrying out a financial transaction or when the AP has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data”. Section 4.4 specifies that enhanced due diligence must be undertaken in cases where there are suspicions of money laundering or terrorist financing.

418. Despite the reference in the circular to business relationships, the institutions themselves indicated that they were not authorised to open accounts for any customers, and that they worked purely on a transactional basis, if necessary having to undertake repeat CDD for regular customers.

Required CDD measures

All institutions covered by PMLA

419. Rule 9(1) of the 2005 PML Rules required institutions to verify the identity, current address, nature of business and financial status of the customer. Rule 9(2) described the specific type of documentation that was needed to fulfil this obligation with respect to individuals, while sub-rules (3)-(6) addressed different categories of customers, specifically, companies, partnerships, trust and unincorporated associations or bodies of individuals. The range of source documents listed for other than individuals is relatively comprehensive. In the case of a natural person, it required “one certified copy of an officially valid document containing details of his permanent address or addresses, current address or addresses, and one copy of his recent photograph and such other documents, including in respect of the nature of business and financial status of the client, as may be required by the banking company or the financial institution or the intermediary, as the case may be”. In November 2009, Rule 9(2) was amended to clarify that the official document must contain details of the customer’s “identity and address”, while exemption from the requirement to obtain a recent photograph was granted in the case of occasional transactions (*i.e.* wire transfers and transactions falling below INR 50 000 or USD 1 000).

420. With respect to legal persons, Rule 9(3) of the PML Rules requires the institution to obtain a certified copy of the following documents:

- a. Certificate of Incorporation;
- b. Memorandum and Articles of Association;
- c. a resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and
- d. an officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

421. The November 2009 amendment to the PML Rules introduced a requirement that, where the client is a “juridical person”, the institution must verify that the person purporting to act on behalf of the client is authorised to do so, and that the identity of that person must be verified.

422. In the case of trusts, certified copies of the following are required:

- a. registration certificate;
- b. trust deed; and
- c. an officially valid document in respect of the person holding an attorney to transact on its behalf.

423. While these provisions clearly require evidence that the customer is properly authorised to act on behalf of the legal person or arrangement, there is no specific provision within the Rules that obligates an institution proactively to determine whether an individual customer is acting on behalf of an undisclosed person, and then to take measures to verify the identity of that person. This obligation is merely implicit within the definition of a “client” which “includes a person on whose behalf the person that engages in the transaction or activity is acting”. This does not adequately address the circumstances in which the customer may not openly disclose that he/she is acting on behalf of another, and the issue is not developed further in the sector-specific guidelines.

Institutions supervised by the RBI (except AMCs)

424. The requirements in the PML Rules are, to varying degrees, repeated, illustrated and expanded upon through the sector-specific guidelines. For example, the RBI Master Circular breaks down the type of documentation considered appropriate for verifying (i) the legal name and other names used, and (ii) the correct permanent address.

Securities sector

425. The SEBI Master Circular also repeats and expands upon the detail of the PML Rules. One specific development, specific to the securities sector, involves the mandatory use of a single identifier. With effect from 2 July 2007, a system was introduced into the securities market whereby every client was required to have a Permanent Account Number (PAN) issued by the tax authorities. Since that date, the PAN has become the sole identification number for persons participating in the securities market. The validity of the PAN can be checked online with the tax authorities by the intermediary. Failure to upload the PAN prior to trading for a client attracts a fine of INR 1 000 (USD 20) per day.

Insurance sector

426. The IRDA circular provides further guidance on the types of identification documentation that would be appropriate for different classes of customer.

Authorised Money Changers

427. The RBI circular for AMCs specifies that photocopies of the identification data need not be retained for transactions below USD 200, and that those for transactions in the range USD 200-2 000 need only be retained for one year. There are also a number of other concessions for low value transactions. The purchase of foreign exchange against payment in cash in INR by the institution may only be done up to a limit of USD 1 000 for residents and USD 3 000 for non-residents (with all transactions made in the same calendar month having to be treated as a single transaction). In all other cases, payment must be made by cheque or demand draft. When the transaction is being undertaken by a non-resident and it exceeds the thresholds for currency declaration at the border (*i.e.* the USD 5 000 and USD 10 000 limits), the institution is required under the FEMA provisions to have sight of a copy of the currency declaration form submitted to the customs authorities. In addition, non-residents are required to show a valid entry visa in their passport. As regards currency sales, customers are required to submit their passport and travel ticket, together with authorisation from their employer if the foreign exchange is required for business travel. Any payment in excess of INR 50 000 (USD 1 000) must be made by the customer in the form of a cheque or

debit/credit card issued in the name of the purchaser. Where the AMC is establishing a business relationship with an entity, it must obtain and verify suitable documents in support of the name, address and business activity, together with a list and identification documents of employees who are authorised to transact business on behalf of the entity.

428. Section 4.3 of the November 2009 circular states that institutions must have procedures in place to identify when a customer is permitted to act on behalf of another person/entity.

Beneficial ownership

All institutions covered by PMLA

429. Prior to the November 2009 amendment to the PML Rules, both the PMLA itself and the Rules were silent on the question of the need to identify the beneficial ownership of funds. However, the amendments to the Rules in that month introduced a requirement, under section 9(1A), that institutions must identify the beneficial owner and take reasonable steps to verify his/her identity. In addition, the amendment introduced a general obligation to obtain information on the purpose and intended nature of the business relationship. The November 2009 Rules did not contain any definition of what constitutes a beneficial owner, but an amendment was issued on 12 February 2010 (the last day for inclusion in this report under the “two month rule”) to provide a definition of the beneficial ownership which exactly matches that of the FATF (*i.e.* it provides no clear guidance on what constitutes ultimate ownership or control).

Institutions supervised by the RBI (except AMCs)

430. Section 2.4(a) of the RBI Master Circular requires banks, in the case of customers that are legal persons or entities, to “understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person”. This section also references the need to take reasonable measures to verify the identity of the beneficial owner, and to establish the purpose and the intended nature of the banking relationship. Section 2.5(ii) states that “banks should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management”. No additional guidance is provided on how institutions are expected to implement the high level requirement contained in the PML Rules.

431. The circular also addresses the issue of client accounts opened by professional intermediaries. It establishes the principle that, whether such accounts are held on behalf of a single client or are “pooled” accounts, the financial institution must look through to the beneficial owners of the funds. The circular goes on to state that where, in such case, the institution relies on the CDD undertaken by the intermediary, it should satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the CDD requirements. However, as explained below (“Implementation and effectiveness”) there appears to be a fundamental problem with the maintenance of such accounts, given the client confidentiality provisions that apply to lawyers, accountants and company secretaries, who routinely open such accounts.

Securities sector

432. Section 5.1 of the SEBI Master Circular emphasises in several places the requirement to identify the beneficial ownership of a securities account, and defines such ownership as “the natural person or persons who ultimately own, control or influence a client and....it also incorporates those persons who exercise ultimate effective control over a legal person or arrangement”. This section also requires the verification of the identity of the beneficial owner. Section 5.5 specifies that firms must establish the purpose and intended nature of the business relationship, but there is no obligation to understand the ownership and control structure of the client. Although the Master Circular makes no explicit reference to the need to understand the ownership and control structure, this requirement is embedded in other rules and

circulars issued by SEBI in previous years as part of the general documentary requirements for trading. In particular, a 1997 regulation defines “control” to “include the right to appoint majority of the directors or to control the management or policy decisions exercisable by a person or persons acting individually or in concert, directly or indirectly, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements or in any other manner”.

Insurance sector

433. The IRDA Master Circular makes no additional references to the need to establish beneficial ownership, to understand the ownership and control structure, or to establish the purpose and intended nature of the relationship. However, an amendment introduced on 3 February 2010 requires that the identity of the beneficial owner be established and that reasonable measures be taken to verify the identity. The definition provided of the beneficial owner goes no further than that provided in the PML Rules.

Authorised Money Changers

434. There were no provisions dealing with beneficial ownership in the March 2009 AMC circular. The circular issued in November 2009 states that the beneficial owner should be identified and all reasonable steps should be taken to verify his identity. It also requires that the purpose and intended nature of the relationship should be established. There is no definition of what constitutes a beneficial owner (this having subsequently been addressed by the February 2010 amendment to the PML Rules), although section 4.4 does specify that the institution should identify the natural persons who ultimately control the legal person.

Ongoing due diligence

All institutions covered by PMLA

435. Prior to the November 2009 amendment to the PML Rules, both the PMLA itself and the Rules were silent on the issue of ongoing due diligence. However, the amendments, under Rule 9(1B), introduced a specific provision that requires institutions to “exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions to ensure that they are consistent with their knowledge of the customer, his business and risk profile”. Provisions were previously made in the regulatory circulars alone.

Institutions supervised by the RBI (except AMCs)

436. Section 2.3(b) of the RBI Master Circular requires banks to prepare a risk-based customer profile for each new customer, containing information relating to the customer’s identity, social and financial status, nature of business activity, etc. Section 2.4(c) provides that banks should periodically update the customer identification data after the account has been opened, indicating that this should take place no less than once every five years for low risk customers, and no less than once in every two years for high and medium risk customers. Section 2.7 includes a requirement to have a risk-based procedure for monitoring accounts to ensure that institutions have an understanding of the customer’s normal and reasonable activity, so that they may be able to identify transactions that fall outside the normal pattern of activity.

Securities sector

437. Section 5.1(e) of the SEBI Master Circular requires firms to “conduct ongoing due diligence and scrutiny, *i.e.* perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary’s knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer’s source of funds”. Unlike the RBI circular, the SEBI document makes no

reference to the need to update client information on a regular basis to ensure that the account monitoring system is soundly based, except in high risk situations (section 5.2.1(b)), where “regular” updates are required. However, both the NSE and the BSE issued circulars³² in 2006 requiring their members to review their client information periodically, and to update their databases to ensure completeness and accuracy.

Insurance sector

438. Section 3.1.1(vii) of the IRDA Master Circular states that verification of identity should be undertaken, not only at the time of the initial contract, but also at the payout stage, and at other times when additional top-up remittances are inconsistent with the customer’s known profile. Subsequently, in its circular of 24 August 2009, the IRDA elaborated on this by stating that “any change in the customer’s recorded profile which comes to the notice of the insurer and which is inconsistent with the normal and expected activity of the customer should attract the attention of the insurer for further ongoing KYC purposes”. Unlike the circulars issued to the banking and securities sectors, there is no general requirement for insurers to undertake regular reviews to ensure that their records are up to date. Instead, the process is driven by the occurrence of specific events (e.g. top-ups and payouts).

Authorised Money Changers

439. Section 4.4 of the November 2009 circular specifies that Authorised Persons should introduce a system of periodic updating of customer identification data (including photograph) if there is a continuing business relationship, and that they should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, its business and risk profile.

Customer risk

All institutions covered by PMLA

440. Neither the PMLA nor the implementing Rules provide explicitly for a risk-based approach to CDD. However, this is a feature incorporated into all the regulatory circulars.

Institutions supervised by the RBI (except AMCs)

441. Section 2.3 of the RBI Master Circular requires banks to develop a customer acceptance policy, one feature of which is the preparation of customer profiles based on risk categorisation. Section 2.3(c) provides illustrative examples of both high and low risk customers, and requires that “intensive” due diligence measures be applied for higher risk customers, examples of which include non-residents, high net worth individuals, trusts, charities, NGOs, companies having close family shareholding, firms with sleeping partners, PEPs, non-face-to-face customers, and “those with dubious reputation as per public information available”. While the guidelines do not provide any specific indication of what additional measures should be applied with respect to high risk customers, section 2.4(a) states that the essential test is for banks to be able to satisfy the competent authorities that the procedures adopted were consistent with the risk profile.

442. In the case of low risk customers, the examples provided include salaried employees whose salary structures are well defined, people belonging to lower economic strata of society whose accounts show small balances and low turnover, government departments, government-owned companies, regulators and statutory bodies. In such cases, “only the basic requirements of verifying the identity and location of

³² Under the rules of both exchanges, the contents of the circulars are mandatory and enforceable, with a range of penalties for non-compliance, including financial sanctions and revocation of membership, which would prevent a broker from practicing. The discussion under Recommendations 5 and 17 describes the extent to which these sanctions have been applied.

the customer are to be met”, although no further elaboration is provided on what actually constitutes such “basic requirements”. In addition, special provision has been made for low income customers under section 2.6 of the guidelines, which provides for opening accounts for those persons who intend to keep balances not exceeding INR 50 000 (about USD 1 000) in all their accounts taken together, and where the total credits in all the accounts taken together is not expected to exceed INR 100 000 (USD 2 000) in a year. In such cases, if a person who wants to open an account is not able to produce the normal documents mentioned in the Master Circular, banks are expected to open an account, subject to:

- a. introduction from another account holder who has been subjected to full KYC procedure. The introducer’s account with the bank should be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer; or
- b. any other evidence as to the identity and address of the customer to the satisfaction of the bank.

443. The guidelines do not provide any specific override for the low risk procedures in the event that there are suspicions of money laundering or terrorist financing, or where external factors might indicate a higher risk³³.

Securities sector

444. Sections 5.2.1(b)-(c) and 5.3.1 of the SEBI Master Circular require firms to classify their clients into three levels of risk (low, medium and high) and to determine the appropriate CDD measures on the basis of the perceived risk. Enhanced CDD measures are prescribed for high risk categories of customers, although no indication is given as to what this might involve. The list of “special category” customers, who are deemed to fall into the higher risk category, is broadly similar to that in the RBI circular, but does also extend to companies making foreign exchange offerings, and clients in high risk jurisdictions, which are defined to include narcotics producers, countries where corruption and fraud is prevalent, sponsors of international terrorism, offshore financial centres and tax havens.

445. While the circular clearly provides for low risk scenarios, there is no guidance as to the circumstances under which this might be appropriate, nor is there any indication of what reduced measures might be possible. On the other hand, section 5.5 makes it clear that, irrespective of the risk, no exemption is possible, for any class of client, with respect to the minimum information and documentation specified in the PML Rules.

446. The guidelines do not provide any specific override for the low risk procedures in the event that there are suspicions of money laundering or terrorist financing, or where external factors might indicate a higher risk.

Insurance sector

447. The requirements and examples of high and low risk customers in the IRDA Master Circular are very similar to those in the equivalent RBI document. There is, however, specific provision for low value transactions. While the basic principle is established that insurers must obtain at least the documentation specified in the circular for all customers, section 3.1.1(ii) of the circular states that “the degree of due diligence to establish KYC could be decided by the insurers where premium is below INR 1 lakh (INR

³³

The authorities are of the opinion that there is no such concept of “simplified due diligence” in India, because a minimum level of due diligence required in all cases. The assessors believe that the provisions do allow for the broader components of CDD to be omitted in certain cases (i.e. beyond simple identification and verification).

100 000 or USD 2 000) per annum”. This is above the EUR/USD 1 000 threshold cited by the FATF as a possible basis for low risk categorisation in the insurance sector, and, according to the practitioners, the vast majority of their business falls below the INR 100 000 threshold. However, there remains an overarching requirement in section 3.1.1 that insurers must obtain documentation sufficient to establish clearly the identity of the customer. This includes an official form of identity document, address and photograph. In the case of transactions above INR 100 000 the insurer must also obtain evidence of the source of funds through the submission of documentary evidence. An exemption is provided from the need to obtain a photograph and proof of address where the annual premium does not exceed INR 10 000 (USD 200) per annum.

448. As a specific risk mitigant, section 3.1.8 of the Master Circular prohibits the receipt of cash payment of premiums in excess of INR 50 000 (USD 1 000) and advises insurers that they should consider setting a lower threshold over time. This requirement has been in place since 2006.

449. Section 3.1.4 of the Master Circular provides a list of products that have been excluded from the AML requirements on the basis of a vulnerability analysis. These include medical insurance, reinsurance and group insurance issued to a company, financial institution or association. However, the exemption also extends to term life insurance contracts “in view of the absence of cash surrender value and stricter underwriting norms for term policies (especially those with large face amounts)”. While such products may, indeed, be low risk and verification procedures are required of the beneficiaries at the payout stage, the FATF standard does not envisage a complete exemption from the CDD requirements in such cases at the time that the business is first written.

450. As is the case with the RBI and SEBI circulars, the IRDA guidelines do not provide any specific override for the low risk procedures in the event that there are suspicions of money laundering or terrorist financing, or where external factors might indicate a higher risk.

Authorised Money Changers

451. Section 4.3 of the circular for Authorised Persons simply states that the nature and extent of due diligence will depend on the risk perceived by the AP.

Timing of verification

All institutions covered by PMLA

452. The original PML Rules required that the client's identity must, in principle, be established at the time of opening the account or executing the transaction, but provided that, if this is not possible, identification may be completed "within a reasonable time" after the account has been opened, or the transaction has been executed. The amendment to the Rules introduced in November 2009 did away with the timing concession, and imposed a hard rule to require CDD at the time of the commencement of a business relationship.

Failure to satisfactorily complete CDD

All institutions covered by PMLA

453. There are no relevant provisions in either the PMLA or the implementing Rules.

Institutions supervised by the RBI (except AMCs)

454. Sections 2.3(a)(iv) and 2.8 of the RBI Master Guidance specifies that a bank must not open an account (or must close an existing one) when it is unable to apply appropriate CDD measures “due to non-co-operation of the customer or non-reliability of the data/information furnished to the bank”. There is no

requirement to consider filing a STR in such circumstances. The RBI indicated that it allows banks discretion over the timing and circumstances under which an account should be closed.

Securities sector

455. The basic requirement specified in various SEBI circulars is that an account must not be opened until the CDD measures have been completed. Section 5.1.2(d) of the Master Circular is specific in laying down certain circumstances in which an intermediary must not open an account for a customer. These include cases where it is not possible to ascertain the identity of the client, information provided to the intermediary is suspected to be false, or where there is a perceived lack of co-operation from the client in providing full and complete information. In such circumstances the intermediary is also required to file a suspicious activity report, and to consider whether the circumstances warrant consultation with relevant authorities in order to determine whether to freeze or close the accounts.

Insurance sector

456. Section 3.1.2(i) of the IRDA Master Circular states that the CDD procedures must be completed satisfactorily before any new insurance contract is issued. While there is no obligation to consider filing a STR when the CDD cannot be completed, the list of indicators for filing such reports (attached to the circular) includes circumstances where the customer insists on anonymity, is reluctant to provide identifying information or provides minimal, seemingly fictitious information. However, the indicators do not have mandatory application. There is no obligation to take specific measures when the insurer can no longer be satisfied that it knows the true identity of the customer.

Authorised Money Changers

457. There were no provisions dealing with the failure to complete the CDD process in the AMC circular of March 2009, but the November 2009 version specifies that the institution must not “undertake any transaction where the AP is unable to apply appropriate customer due diligence measures *i.e.* AP is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non-co-operation of the customer or non-reliability of the data/information furnished to the AP”. It states further that “when a business relationship is already in existence and it is not possible to perform customer due diligence on the customer in respect of business relationship, APs should terminate the business relationship and make a Suspicious Transaction Report to the FIU-IND”.

Existing customers

All institutions covered by PMLA

458. There are no relevant provisions in either the PMLA or the implementing Rules to address the issue of how to deal with customers who were on the institutions’ books prior to the introduction of the current CDD standards.

Institutions supervised by the RBI (except AMCs)

459. There is no explicit requirement in the RBI’s Master Circular to apply the current CDD standards in their totality to existing customers. However, section 2.4(c) states that banks should update customer identification data (including the photograph) on a regular basis, although the scope of such data would almost certainly be less than a full CDD process. The period for such reviews should not exceed five years for low risk customers and two years for high risk customers. The circular does not specify the need for renewed CDD in the event of certain trigger events. However, the circular issued to the non-bank financial institutions on 1 July 2009 is more specific on this issue. It states that institutions should apply the same standards to existing clients as for new clients, based on materiality and risk. In addition, it states that any unusual pattern in the operation of an existing account should trigger a review of the CDD measures.

460. The RBI has indicated that there is no reference to pre-existing accounts in the July 2009 circular because institutions were required, under an earlier circular issued at the time of the introduction of the PML Rules, to review all accounts by end-2005 and to acquire fresh ID documents and a photograph. If verification of the legacy accounts could not be completed, institutions were expected to freeze them until such time as the customers provided the required information. The banks reported that, with respect to those frozen accounts that are considered to relate to higher risk customers, they have adopted the practice of giving 30 days notification of closure. The number of accounts that have not been updated is relatively high in the NBFC sector, and the RBI has issued instructions that appropriate CDD must be done prior to the disbursement of any funds.

Securities sector

461. The SEBI Master Circular makes no reference to the need to revisit the CDD on existing customers. However, in January 2008 an instruction was given to the Depositories to freeze all accounts for which a PAN had not been obtained, following the introduction of the PAN as the unique identifier in July 2007. At that time, this action affected 4 million accounts, but by the time of the on-site visit this number had been reduced to just less than 600 000. In addition, the rules of the exchanges require their members to review client identification data regularly and to update it as necessary.

Insurance sector

462. Section 3.1.2(ii) of the IRDA Master Circular states that the CDD requirements should be applied retrospectively to all contracts entered into since 1 January 2006. This date was originally set at 1 April 2004, but the IRDA agreed to bring it forward after representations from the industry about the scale of the task being imposed on the insurers. This procedure is not required for any policy for which the annual premium is less than INR 100 000 (USD 2 000) per annum. There are no other requirements with respect to policies that pre-date 1 January 2006.

Recommendation 6 (Politically Exposed Persons)

All institutions covered by PMLA

463. There are no relevant provisions relating to PEPs in either the PMLA or the implementing Rules.

Institutions supervised by the RBI (except AMCs)

464. Section 2.3(a)(ii) of the RBI Master Circular specifies PEPs as an example of a class of customer that might fall into the highest risk category. Section 2.5(iv) provides a definition of a PEP that matches that of the FATF and relates only to foreign persons (although the banking sector indicated that it tends to apply the principle also to domestic PEPs). For such cases, banks are required to check what information is available in the public domain; seek information on the source of funds (but not overall wealth); ensure that the decision to open the account is taken at a senior level; and subject the account to enhanced monitoring. A supplement to the Master Circular issued on 11 September 2009 adds that, in the event that a customer or the beneficial owner of an existing account subsequently becomes a PEP, senior management approval should be obtained for the continuation of the relationship, and the account should be subject to all the measures specified for PEPs, including enhanced due diligence.

465. Despite these measures, there is no overall requirement to implement specific risk management procedures for identifying PEPs, either at the time that an account is opened or in the course of an existing business relationship. The obligations appear to be reactive rather than proactive. In addition, while

reference is made to the risks associated with close relatives of PEPs, this is only a cautionary guideline and does not represent an obligation to apply specific measures to such clients³⁴.

Securities sector

466. Section 5.4(e) of the 2008 SEBI Master Circular identifies foreign PEPs as “clients of special category”. There is no definition of what constitutes a PEP, but this is addressed through a supplementary circular issued on 1 September 2009 (subsequently consolidated into the revised Master Circular of 12 February 2010), which incorporates the same definition as used in the RBI circular, except that it extends the enhanced CDD requirements to family members. Section 5.5 of the Master Circular requires that intermediaries should put in place necessary procedures to determine whether an existing or potential customer is a PEP; to seek additional information in such cases; to obtain senior management approval for any new or existing account identified as belonging to a PEP; and to verify the source of funds (but not wealth). Section 5.2.1 requires that “clients of special category” be subject to “a higher degree of due diligence (including ongoing monitoring) and regular update of KYC profile.

Insurance sector

467. Section 3.1.3(ii) of the IRDA Master Circular identifies PEPs among a broad group of customers who present high risk profiles. PEPs are not defined and there is no indication of whether the term includes or excludes domestic PEPs. In the case of all high risk customers, insurers are required to apply enhanced due diligence, but are only “advised to carry out the appropriate level of due diligence keeping the observations at 3.1.5 in view”. Section 3.1.5 indicates that insurers should document the customer’s source of funds and estimated net worth, but the language linking these two sections is vague and does not seem to impose a specific obligation. The supplementary amendments to the circular, issued on 24 August 2009, specify that insurers must put in place procedures to ensure that all contracts with high risk customers are subject to approval by senior management. This is defined to be at least the head of underwriting or the chief risk officer. There are no specific references to the need to have in place procedures for identifying customers as PEPs, for enhanced monitoring of the accounts, or for taking action with respect to accounts of which PEPs are the beneficial owners.

Authorised Money Changers

468. The November 2009 circular provides a definition of a PEP which matches the concept in the FATF standards. It requires that APs should gather sufficient information on any person/customer of this category intending to undertake a transaction or establish a business relationship, and check all the information available on the person in the public domain. APs are required to verify the identity of the person and seek information about the source of wealth and source of funds before accepting the PEP as a customer. The decision to undertake a transaction with a PEP should be taken at a senior level, which should be clearly spelt out in Customer Acceptance Policy. APs should also subject such transactions to enhanced monitoring on an ongoing basis. It is discretionary as to whether the same procedures are applied to transactions with the family members or close relatives of PEPs. The language also appears initially to be discretionary when stating that “the above norms may also be applied to customers who become PEPs subsequent to establishment of the business relationship”, but then it goes on to state that “where a customer subsequently becomes a PEP after a business relationship has already been established, enhanced CDD should be performed on such customers and decision to continue business relationship with the PEP should be taken at a sufficiently senior level”.

³⁴ The authorities maintain that all the components of the regulatory circulars are mandatory, regardless of the actual language used (e.g. “may” compared with “should” or “must”). The assessors cannot accept this, given that some of the statements in the circulars are clearly intended to be discretionary.

Recommendation 7 (Correspondent banking)

469. Section 2.12(a) of the RBI Master Circular defines correspondent banking and provides examples of the services that may be provided under such an arrangement. It then proceeds to mirror very closely the language underpinning the requirements of Recommendation 7, specifically stating:

“Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank’s management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent’s/respondent’s country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing ‘due diligence’ on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.”

470. There is no evidence that Indian financial institutions provide other types of facility similar to a cross-border banking relationship. The RBI has not undertaken any targeted inspections to establish whether the banks are complying with the requirements for correspondent banking, and this aspect of banks’ business does not appear on the checklist for AML/CFT compliance attached to the RBI inspection manual.

Recommendation 8 (Technological developments and non-face-to-face transactions)

Institutions supervised by the RBI (except AMCs)

471. Section 2.10 of the RBI Master Circular states that “banks should pay special attention to any ML threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in ML schemes”. The section provides further instruction on measures required in respect of credit and electronic transfer cards, stressing the need to ensure proper due diligence is performed on all those, including supplementary care holders, that have access to the facility. Separate guidance (including relating to AML/CFT protection) has been issued with respect to mobile banking and credit/debit card transactions. Unlike in some countries where mobile banking is developing outside the mainstream banking sector, in India the authorities have restricted its use to that of a communication platform only, so that banking institutions must be involved directly at both ends of each transaction.

472. As regards non-face-to-face relationships, section 2.5(v) specifies that, in addition to the normal CDD measures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all documents is required, and it is suggested that banks may also require the first payment to be made through the customer’s account with another bank which adheres to appropriate CDD measures. In the case of cross-border relationships, the circular indicates that banks may have to rely on third party certification, but only when the introducer is regulated and supervised, and has proper CDD processes. However, the general perception among the financial institutions is that, with the exception of

non-resident Indians, all potential account-holders must present themselves in person to fulfil the identification and verification procedures. Therefore, the institutions regard the non-face-to-face provisions as largely being academic.

Securities sector

473. Technological developments such as internet trading and Direct Market Access (DMA) have been allowed by SEBI subject to fulfilment of certain safeguards. Guidelines for internet trading were issued on 31 January 2000, and for direct market access on 3 April 2008.

474. In its Master Circular (section 5.4) SEBI has included non-face-to-face customers in the list of “clients of special category”. Consequently, under section 5.2.1(b) intermediaries must undertake enhanced due diligence on such accounts, including a regular update of the customer profile. However, in contrast to the provision in the Master Circular, SEBI issued a directive on 2 July 2008 specifying that “it will be the responsibility of stockbrokers to ensure in-person verification by its own staff while registering a client under KYC norms”. A similar obligation has been imposed on the depository participants. This includes clients who wish to engage in trading via the internet, and it requires that either the client must present himself at the intermediaries’ office, or the intermediary must send a member of staff to visit the client. Non-face-to-face transactions are permitted only in respect of Non-Resident Indians (NRI), and sub-accounts of Foreign Institutional Investors (FIIs). SEBI specified norms relating to ‘in-person verification’ of accounts of non-resident Indians on 4 April 2008. In such cases intermediaries are required to obtain KYC documents attested by any one of the following entities - notary public, court, magistrate, judge, local banker, or the Indian Embassy/Consulate General in the country where the client resides. It is unclear how this earlier requirement, apparently prohibiting non-face-to-face account opening, relates to the contents of the Master Circular.

Insurance sector

475. The IRDA Master Circular provides no specific guidance on technological developments. It does provide that due diligence measures applicable to non-face-to-face customers are the same as those applicable to face-to-face customers, except that the documentation requirements should be completed within 15 days of issuance of the policy where the premium per person per annum exceeds INR 100 000 (USD 2 000). According to the insurance companies, less than one percent of their policies are issued to customers on a non-face-to-face basis.

Authorised Money Changers

476. Section 4.9 of the November 2009 circular addresses the broad issue of technological developments, but also refers specifically to the issuance, by certain authorised dealers of foreign currency denominated pre-paid cards to travellers going abroad. It specifies that institutions should ensure compliance with all the guidelines, and that the issuers should also consider undertaking CDD on other institutions that market the cards on their behalf.

Implementation and effectiveness

477. The institutions with which the assessment team met had a high level of appreciation of the PMLA, the accompanying Rules and the circulars issued by the competent authorities. In some respects, the degree of familiarity with the range of requirements was surprising, especially among the small co-operative banks, which might typically be less well informed about those aspects of the regulations that do not directly impact their business. Although some of the CDD requirements are relatively new, the regulatory authorities have been undertaking examinations for some time to help establish the level of compliance in each of the sectors. These examinations appear to show a relatively good level of compliance, based on the perception that the regulatory inspection procedures are extensive, detailed and

rules-based. However, as the following table shows, there continue to be weaknesses in the co-operative banking sector, as might have been expected, but this needs to be put in the context of the structure of the banking sector, where the 84 scheduled banks account for 87.5 percent of the total assets in the system, while the 2 200 co-operative banks account for no more than 11 percent.

Table: Measures taken by the RBI for violation of the KYC guidelines

| Year | Category of agency ³⁵ | Penalties | | Advisory notices | Show-cause notices | Warning letters |
|-------------------------|----------------------------------|--------------------------|-------------------------|------------------|--------------------|-----------------|
| | | No. of agencies involved | Amount (in million INR) | | | |
| 2004-2005 | Scheduled commercial banks | 2 | 1.0 | | 3 | 1 |
| | Urban co-operative banks | | | 52 | | |
| | Authorised money changers | | | | | 1 |
| 2005-2006 | Scheduled commercial banks | 12 | 12.5 | 10 | 13 | |
| | Urban co-operative banks | | | 93 | | |
| | Authorised money changers | | | 1 | 1 | 1 |
| 2006-2007 | Scheduled commercial banks | 2 | 2.0 | 1 | 4 | |
| | Urban co-operative banks | 2 | 1.0 | 77 | 6 | |
| | Authorised money changers | | | | 3 | 1 |
| 2007-2008 | Scheduled commercial banks | 2 | 2.0 | 1 | | |
| | Urban co-operative banks | 11 | 3.8 | 33 | 7 | |
| | Authorised money changers | 1 | 0.005 | | 4 | 2 |
| 2008-2009 (31.12.09) | Scheduled commercial banks | | | 1 | | |
| | Urban co-operative banks | 11 | 3.8 | 106 | 11 | 2 |
| | Authorised money changers | | | 1 | 7 | |

478. The RBI reports that the most common violations that attract penalties relate to the account-opening procedures, transactions monitoring, and weaknesses in the overall internal control procedures.

479. The CDD regime in the securities sector pre-dates the introduction of the PMLA, since it forms part of the market integrity framework. The SEBI notes that it has consistently taken action against intermediaries, by way of suspension and cancellation of the registration certificate, warning, censures and monetary penalties, for matters that related either directly or indirectly to CDD failings. The range of violations for which intermediaries have been penalised include non-maintenance of client database, failure to obtain a proper client registration form, failure to conduct ongoing due diligence on the trading activity of the client (*i.e.* failure to notice that the net worth or income levels of the client do not match up with the client's trading activity). The majority of these cases have been where CDD failures were incidental to an underlying offence (e.g. the Yes Bank initial public offering where failures in CDD allowed fraudulent applications for multiple allocations of shares; and the case in December 2009 when Barclays, a FII, was banned from issuing participatory notes for failing to disclose to SEBI the true identity of the underlying

³⁵ The term "agency" refers to the head office, a branch or other office of a licensed institution.

investors). The IPO case hastened the introduction of the PAN as the obligatory identifier for all clients trading in the market. The following table illustrates the measures taken by the SEBI since 2005 with respect to failings that included CDD deficiencies.

Table: Penalties imposed by SEBI for AML/CFT failings, including CDD deficiencies

| Monetary penalties | | | | | | |
|---|------------------------|------|------|------|---------|--------------------|
| | | 2005 | 2006 | 2007 | 2008 | 2009 (nine months) |
| Adjudication Orders | Number | 6 | 8 | 6 | 1 | 8 |
| | Value (in million INR) | 1.41 | 1.96 | 0.68 | 1 | 2.23 |
| Consent Orders | Number | | | | 5 | 3 |
| | Value (in INR) | | | | 750 000 | 1 400 000 |
| Other sanctions | | | | | | |
| Cancellation | | - | 2 | - | - | |
| Suspension | | 8 | 23 | 13 | 3 | 2 |
| Warning | | 9 | 7 | - | 1 | 2 |
| Censure | | 7 | 10 | 6 | 1 | |
| DPs directed not to open fresh demat accounts | | - | 13 | 1 | - | |
| Total | | 24 | 55 | 20 | 5 | 4 |

480. However, day-to-day supervision of the market participants is devolved to the exchanges, which have their own sanctioning powers. For instance, in recent years the National Stock Exchange (NSE) has sanctioned 64 brokers for not complying with the in-person verification procedures.

481. No formal sanctions have yet been applied in the insurance sector, although the IRDA has identified a range of failings during its on-site examination process. The regulator indicated that the institutions concerned responded positively to its subsequent instructions to remedy the deficiencies, and that no sanctions were ultimately warranted. In August 2007, the IRDA wrote to all insurers highlighting the common failings that it had identified during a focused review of CDD procedures. These included failure to update the CDD for existing customers in line with the current requirements, and inadequate procedures to identify the customers' source of funds. More generally, the IRDA concluded that the CDD procedures being adopted by the industry were broadly in line with what was required, although it identified a range of issues which it did not believe were widespread failings, for example:

- a. Existing customers-documents being collected as and when the settlement of claims is taken up.
- b. No proper due diligence carried out during top-up remittances.
- c. No proper AML checks carried out during assignment to un-related third party.
- d. Acceptance of cash beyond INR 50 000/USD 1 000 through inter-connected multiple transactions.
- e. Company is obtaining Identity/Address Verification statement from its employees as valid document for compliance with KYC requirement.

- f. Reliance on bank documentation rather than getting original.
- g. Multiple transactions not being properly linked.

482. Overall, there is no evidence that there are systematic failings in the implementation of the broader CDD obligations by financial institutions in India, but there are several specific issues which give rise to varying degrees of concern.

- a. **Beneficial ownership:** Neither the PML Rules nor the various circulars promulgated by the respective regulators provide a clear definition of what constitutes beneficial ownership. While the February 2010 amendment to the Rules and the regulatory circulars talk in terms of the natural person who ultimately controls the customer, there is no further guidance on how this should be addressed with respect to corporate clients. As a result the different sectors have developed their own understanding of what is required, either through discussion with their professional associations or through direct dialogue with the individual regulators. In the case of the banking sector, the Indian Banking Association works on the principle that institutions should identify “substantial holdings”, which it defines as falling in the range of 10-25% of the shareholding, but the association has not published any formal guidance. In practice, the banks with which the assessment team met appear to work within the 15-20% range. By contrast, the SEBI expects intermediaries to work to a threshold figure of 5%, while the insurance sector appears to take the view that the issue of beneficial ownership is not material to its business. Generally, institutions held the view that it was sufficient to rely on the information listed on the central company register (which maintains some form of beneficial ownership information to the first level of control - see discussion under Recommendation 33), but there was no expectation that institutions should “drill down” further. Moreover, the procedures adopted appeared not to envisage the need to establish that individuals holding less than the threshold figure might be acting in concert with other shareholders, thereby raising their effective control above the threshold level. There clearly needs to be further clarification from the regulators as to what is expected in the whole area of beneficial ownership.
- b. **Reliability of ID documents:** Considerable reliance is placed, during the CDD process, on a range of official ID documents available to Indian nationals. However, there appear to be concerns among financial institutions and some parts of government about the underlying reliability of the documents. There is currently no single national identity card in India, and residents will have a variety of different forms of documentation. For example, tax payers (who form a relatively small proportion of the population by international comparison) will have a PAN, while low income families may have only a ration card issued to give access to subsidised basic foodstuffs. The assessors were advised that both these cards have been prone to duplication by individuals registering more than once using variations in their names. This is made possible in part because there is no requirement to attend in person to acquire the cards. In addition, in the case of the ration card, the document is issued only to the head of the family, who must attest that any members of the family who rely on the document (including for access to banking facilities) are indeed family members. A similar situation arises in the context of the Hindu Undivided Family, where the PAN is also issued to the patriarch who must attest on behalf of others in the family. The tax authorities have cancelled a significant number of duplicate PANs, and it is now a criminal offence to hold a card in the wrong name. The Government has initiated a project to introduce a unique ID card for all citizens, which it will start to introduce from August 2010. Given the size of the Indian population, this exercise will take some considerable time to complete.
- c. **Pooled accounts for lawyers and accountant:** The use of pooled client accounts is common in the accountancy, legal and company secretary professions, but such accounts are covered by strict professional secrecy provisions which prevent the disclosure to the financial institution

of the name(s) of the beneficial owner(s) of the funds³⁶. For example, section 140 of the accountants' Code of Conduct imposes a general duty on the profession to maintain client confidentiality, except when disclosure is permitted by the client, required by law, or is necessitated by professional duty or right. The accountants' professional body confirmed that disclosure of the names of clients for whom funds were held in a client account would not fall within any of these exclusions. Similarly, the company secretaries' professional body indicated that the maintenance of client accounts by its members was entirely possible, but that the Second Schedule to the Company Secretaries Act prohibits the disclosure of any information acquired in the course of a professional engagement, except with the approval of the client or if compelled by law. Since the accountants and company secretaries are not yet subject to the PMLA, the banks are unable to fall back onto the provisions of section 2.5(iii) of the RBI Master Circular, which allows them to rely on the CDD undertaken by professional intermediaries, but only when the intermediary is subject to adequate AML/CFT requirements. It remains unclear how exactly the financial institutions fulfil their obligation to identify the beneficial owners in such circumstances.

- d. India Post was not brought under the PMLA until June 2009, and this came about purely because it is an Authorised Person in respect of the small amount of foreign exchange business that it does. However, the range of financial services that it offers is extensive (e.g. deposits, mutual funds, life insurance, money remittance), and it is stated to be the largest retail bank in India (with some 220 million small savings accounts). While these accounts are mostly of very small value and may generally be regarded as low risk, there is clearly a significant task ahead for India Post to ensure that its CDD procedures for the very large number of existing clients are brought into line with the PMLA requirements.
- e. Insurance intermediaries: While the IRDA circular firmly places the obligation on the insurer to oversee the activities of the tied agents, the assessors had some concerns about how this is achieved in respect of the basic customer identification procedures. The primary responsibility for the initial identification rests with the agent, who is required to take copies of the original documentation on which he/she relied. Further copies are then forwarded to the insurer. However, the original copies do not have to be notarised by an independent professional, and at best they may be attested by the insurers' regional development officers, who visit the agents from time to time. These procedures appear to place undue reliance on the professional competence of individual agents.
- f. PEPs: The three regulators have all issued instructions with respect to PEPs, but there are inconsistencies in the scope of what each sector is required to do (e.g. in implementing risk management procedures or applying the measures to close relatives and accounts of which the ultimate beneficial owner is a PEP). Therefore, there can be no comfort that there is a common understanding across the financial industry of what are the full range of obligations.
- g. Non-face-to-face business: There are appropriate provisions in place for the banking and securities sectors, even if these are regarded by the institutions as largely academic with respect to their domestic customer base, because of the general view that all accounts must be opened in person by the customer. The provisions in the insurance circulars are much less robust, in that they fail to mention the need to take special measures to prevent the misuse of technological development, and they offer no material guidance on how to deal with non-face-

³⁶

The authorities maintain that such pooled accounts do not exist, and that all funds held by professional intermediaries on behalf of their clients are held in segregated accounts in the names of the clients. However, the assessors discussed this matter at considerable length with the intermediaries, who were very clear on the issues addressed in this paragraph.

to-face transactions, even though the range of options for remote account-opening is mentioned. This needs to be addressed.

- h. Regulators' circulars: In analysing the obligations imposed on the financial institutions, the assessors had to review in excess of ten sets of core regulatory circulars, together with a far greater number of amendments and supplementary notices. Although there is no indication that the plethora of different circulars issued by the respective regulators (including at departmental level), have an impact on the institutions' understanding of their obligations, there does appear to be some benefit in seeking to rationalise them in order to avoid potential confusion. Currently, there is a range of circulars, all of which have similar messages, but which contain different language and impose marginally different obligations. While some of these differences are entirely reasonable to reflect the different nature of the businesses, others seem simply to reflect different drafting styles or minor variations on a theme adopted by the individual agencies or departments. However, the institutions report that the individual regulators, which adopt primarily a rules-based approach, require strict adherence to their specific circulars for each business unit, which largely prevents institutions with multiple authorisations from implementing a single set of group-wide AML/CFT systems and controls. While there were no reports of this causing any substantive differences of approach between business units, it does generate a degree of inefficiency.

3.2.2 Recommendations and Comments

483. It is recommended that the authorities:

- Bring the commodities futures brokers fully within the scope of the PMLA.
- Amend the PML Rules to:
 - require renewal of CDD when there are suspicions of money laundering or terrorist financing, or where there are doubts about the adequacy or veracity of previously obtained customer identification data; and
 - require institutions proactively to determine whether a customer is acting on behalf of another person.
- Amend the regulatory circulars to:
 - implement a requirement that the low risk provisions should not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not, in fact, pose a low risk (RBI and IRDA);
 - provide guidance on how to interpret the definition of beneficial ownership and on the procedures required to identify the ultimate natural person who owns or controls the customer (all regulators);
 - introduce measures to prevent the opening of client accounts unless the professional intermediary is willing and able to provide information on the beneficial owners (RBI);
 - introduce requirement to understand the ownership and control structure of legal persons (IRDA);
 - introduce a requirement that an institution should consider filing a STR when an institution can no longer be satisfied that it knows the true identity of a customer (RBI and IRDA); and
 - remove the exemption for term life policies from the AML obligations at the time that the policy is first written (IRDA);

- introduce consistent requirements within all three sets of circulars to ensure that all institutions should have appropriate ongoing risk management procedures for identifying (and applying enhanced CDD to) PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.
- Review the procedures under which the insurers are entirely reliant on the basic identification procedures carried out by their agents (IRDA).
- Give consideration to consolidating the regulatory circulars to help ensure consistency of application; to avoid unnecessary variations in the obligations being imposed on institutions that are active in the various sectors; and to allow improved group risk management procedures.

3.2.3 Compliance with Recommendations 5 to 8

| | Rating | Summary of factors relative to s.3.2 underlying overall rating |
|-----|--------|--|
| R.5 | PC | <ul style="list-style-type: none"> ● Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. ● No provisions in law or regulation that require CDD to be renewed when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data. ● No provisions in law or regulation that require an institution proactively to determine whether a customer is acting on behalf of another person. ● Lack of clarity and divergent practices in relation to the identification and verification of beneficial ownership. ● Professional secrecy provisions prevent identification of beneficial owners of client accounts. ● No obligation in IRDA circular to understand ownership and control structures of legal persons. ● The RBI and IRDA circulars do not require a specific override of the procedures for low risk customers when there are suspicions of ML/FT, or where factors suggest that the customer poses a higher risk. ● No explicit requirement in the RBI and IRDA circulars to consider filing a STR when the institution can no longer be satisfied that it knows the true identity of the customer. ● Term life policies exempt from AML requirements at stage of writing the policy. ● Implementation issue: <ul style="list-style-type: none"> ○ recent introduction of the Authorised Persons within the PMLA (including India Post) results in questions over extent of implementation. |
| R.6 | PC | <ul style="list-style-type: none"> ● Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. ● No requirement in the RBI and SEBI circulars to implement ongoing risk management procedures for identifying PEPs. ● No requirement in the RBI circulars to apply enhanced measures to close relatives of PEPs. ● No obligation in the IRDA circular to apply enhanced measures to entities where the beneficial owner of the customer is a PEP. |
| R.7 | LC | <ul style="list-style-type: none"> ● Effectiveness issue: <ul style="list-style-type: none"> ○ no evidence provided that implementation is effective. |
| R.8 | LC | <ul style="list-style-type: none"> ● Inadequate provisions in the IRDA circulars to address the issues of technological developments and non-face-to-face business. |

3.3 *Third parties and introduced business (R.9)*

3.3.1 *Description and Analysis*

Recommendation 9

484. The authorities have indicated that third-party introduced business is not permitted in any sector of the Indian financial community, and this is a view shared by all the institutions with which the assessment team met. However, section 2.5(iii) of the RBI Master Circular does make reference to possible reliance on CDD undertaken by a third party in the context of client accounts opened by professional intermediaries. In such circumstances the bank must satisfy itself that the intermediary is regulated and supervised and has adequate AML systems in place. The circular also specifies that the ultimate responsibility for knowing the customer lies with the bank. However, there is no reference to the need of the financial institution to obtain core CDD information immediately, or to seek assurances that the identification and other data will be made available on request. The circular is also silent on the circumstances (if any) in which an intermediary may be based outside India.

485. As mentioned in the discussion of Recommendation 5, special provision has been made for low income customers under section 2.6 of the guidelines, which provides for opening accounts for those persons who intend to keep balances not exceeding INR 50 000 (about USD 1 000) in all their accounts taken together, and where the total credits in all the accounts taken together is not expected to exceed INR 100 000 (USD 2 000) in a year. In such cases, if a person who wants to open an account is not able to produce the normal documents mentioned in the Master Circular, banks are expected to open an account, subject to:

- a. introduction from another account holder who has been subjected to the full KYC procedure. The introducer's account with the bank should be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer; or
- b. any other evidence as to the identity and address of the customer to the satisfaction of the bank.

486. The assessors are of the opinion that this type of "introduction" is not what is envisaged under Recommendation 9 (as it is primarily to do with overcoming the absence of basic identification documentation), and have, therefore, not taken it into account here.

Implementation and effectiveness

487. Although there appear to be no provisions formally prohibiting third-party introduced business, the universal view among financial institutions is that such business is not permitted, even where the introduction might come from another part of the group. Indeed, the inability to rely on intra-group introductions was mentioned to the assessment team as a common cause of frustration among both institutions and clients, who are required to submit identical documents when taking up different products offered by a single group. There seems to be no clear explanation of why the RBI circular makes reference to the concept of introduced business in these circumstances, and it has been suggested that it is simply the result of "copying and pasting" text from documents produced by the Basel Committee on Banking Supervision and the FATF. After careful consideration, the assessors have concluded that, in both regulation and practice, the terms of Recommendation 9 are not applicable in the case of India.

3.3.2 Recommendations and Comments

488. In view of the potential confusion that might be caused by section 2.5(iii) of the RBI Master Circular, it is recommended that this section be amended to remove all doubt about the scope for institutions to accept business introduced by third parties, as envisaged under Recommendation 9.

3.3.3 Compliance with Recommendation 9

| | Rating | Summary of factors relevant to s.3.3 underlying overall rating |
|-----|--------|---|
| R.9 | N/A | <ul style="list-style-type: none"> This Recommendation is not applicable in India. |

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

Recommendation 4

489. There are no specific financial institution secrecy provisions in the regulatory laws, and the competent authorities have been given a range of powers to enable them to acquire information from institutions.

FIU-IND

490. Section 50 of the PMLA gives the same powers to the FIU-IND as are vested in the civil courts with respect to discovery and inspection, production of documents, producing of evidence, obtaining of witness statements, etc. Section 71 states that the provisions of the PMLA shall have effect notwithstanding anything to the contrary in any other law for the time being in force.

Reserve Bank of India (RBI)

491. Through a circular issued to the banking sector on 11 February 2008, the RBI confirmed that the scope of the secrecy law in India has generally followed the common law (Tournier) principles. The bankers' obligation to maintain secrecy arises out of the contractual relationship between the banker and customer, and as such no information should be divulged to third parties except under circumstances which are well defined such as:

- a. where disclosure is under compulsion of law;
- b. where there is a duty to the public to disclose;
- c. where interest of bank requires disclosure; and
- d. where the disclosure is made with the express or implied consent of the customer.

492. However, the RBI has broad powers, under its own governing legislation and the various laws that it administers, to require institutions to provide whatever information it may require, and to carry out inspections with the right of access to all records held by the institutions.

Securities and Exchange Board of India (SEBI)

493. The SEBI has specified through its circular issued on 8 November 2001 that the member client agreement between a stock broker and clients shall contain a clause to the effect that "the member hereby undertakes to maintain the details of the client, as mentioned in the client registration form or any other information pertaining to client, in confidence and that he shall not disclose the same to any person/entity except as required under the law".

494. Under section 11 of the SEBI Act and respective regulations governing the functioning of securities markets intermediaries, the SEBI is authorised to call for any information from any of its stock exchanges, mutual funds, and other persons associated with securities market intermediaries and self-regulatory organisations. Additionally, they are able to access any information of publicly listed companies and share this information for financial investigation purposes.

Insurance Regulatory and Development Authority (IRDA)

495. The IRDA is empowered under section 14(2)(h) of the IRDA Act to call for information from insurers, intermediaries, insurance intermediaries and other organisations connected with the insurance business. This section is very general in its scope, but section 33 of the Insurance Act is far more specific, as it imposes an obligation on insurers to produce all such books of accounts, registers and other documentation as the inspector may request.

Implementation and effectiveness

496. The routine reporting requirements imposed on financial institutions are extensive, as are the powers granted to the competent authorities to request, or have access to, such additional information as they may require. Discussions with the financial institutions indicated that they consider that they have an obligation to submit whatever information may be requested by the authorities, and that they are not inhibited from so doing by any statutory provisions.

3.4.2 Recommendations and Comments

497. There are no recommendations in relation to Recommendation 4.

3.4.3 Compliance with Recommendation 4

| | Rating | Summary of factors relative to s.3.4 underlying overall rating |
|------------|---------------|---|
| R.4 | C | This Recommendation is fully observed. |

3.5 Record-keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10 (record-keeping)

498. The record-keeping regime established under the PMLA and the PML Rules requires transaction, customer identification, and account records to be maintained for ten years. Prior to the February 2010 amendment to the PML Rules, the record-keeping regime did not cover all necessary records, nor did it require records to include all the information specified by the FATF standard. The 2010 amendments to the PMLA Rules greatly expand the scope of required transaction records, but otherwise do not address Recommendation 10's criteria (e.g., the amendments do not alter the record-keeping requirements for customer identification or account records). As noted above, the PML Rules were amended on 12 February 2010, precisely two months after the end of the on-site visit, and therefore, these amendments to the PML Rules cannot be considered in assessing the effectiveness of India's record-keeping requirements, since they were not implemented during the relevant timeframe. Accordingly, in order to accurately evaluate India's record-keeping system during the relevant period, the discussion below examines the legal framework and implementation that existed prior to the February 2010 Amendments, as well as assesses the (limited) changes in record-keeping requirements established by the PML Amendment Rules against Recommendation 10's criteria. It should also be noted that the PMLA did not cover India Post until June 2009.

All institutions covered by PMLA

499. Section 12 of the PMLA requires covered institutions to maintain proper records of all transactions, the nature and value of which is to be prescribed, and customer identification records. It also establishes a ten-year retention period for these records, dating from the “cessation of the transactions between the client and the covered institution”.

500. The PML Rules repeat the ten-year retention period for both transaction and customer identification records, calculated as in the PMLA, “from the date of cessation of the transactions between the client and the institution”.

501. This timeframe is acceptable for transaction records, which Recommendation 10 requires to be maintained for at least five years following the completion of the transaction. However, as applied to customer identification records and account files, it is not clear that the PMLA’s formulation of when the retention period begins complies with the FATF standard. Recommendation 10 specifically requires the record retention period for customer identification records to be five years following the termination of an account or business relationship, not the cessation of the transactions with the client. The PMLA and PML Rule’s “cessation of the transactions” language could be interpreted to mean that the retention period for customer identification records runs from the date of the last transaction with the customer. As a theoretical matter, this could allow in certain circumstances (where an account is inactive for over five years but has not been closed) for a shorter record retention period than the FATF standard contemplates. As a practical matter, however, the PMLA’s formulation would not create a gap, at least in the banking sector, since bank accounts not operated for a continuous period of more than two years by the customer are treated as dormant, and if the account holder still does not operate the account for another year, the bank account is classified as inoperative. Thus, three years after the last customer transaction, a bank account would be closed. Regardless of the precise formulation of the trigger, India’s ten-year record retention period, together with account closure three years after the last transaction, ensures that in the banking sector, customer identification and account records are maintained for at least five years following termination of the business relationship.

502. The PML Rules define “transaction” to include the deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by check, payment order or other instruments or by electronic or other non-physical means. Until the February 2010 PMLA Amendments, Rule 3 of the PML Rules required transaction records to be maintained only for:

- a. cash transactions (deposits and withdrawals) above INR 1 million (USD 20 000)—including series of integrally connected cash transactions occurring within a month that together exceed the INR 1 million threshold;
- b. cash transactions using forged or counterfeit currency notes; and
- c. suspicious transactions, whether or not made in cash.

503. Rule 4 of the pre-2010 PML Rules provided that the required transaction records must include the nature of the transaction; the amount and currency in which the transaction was denominated; the transaction date; and the parties to the transaction.

504. For transaction records, the PML Rules as they existed until 12 February 2010 had important gaps with respect to both the types of transactions covered and the information required. The PML Rules established an INR 1 million (USD 20 000) threshold for cash transaction records that was inconsistent with Recommendation 10, which requires financial institutions “to maintain *all* necessary records on transactions, both domestic and international”, without any threshold limitation. In addition, for non-cash transactions, the PML Rules only required record-keeping for *suspicious* transactions. The failure to

require record-keeping for all transactions, whether or not considered suspicious, fell significantly short of the criteria set forth under Recommendation 10. Moreover, while the PML Rules specified that transaction records should contain many of the components necessary to permit reconstruction of individual transactions, they did not require transaction records to include the account type and identifying number.

505. The PML Amendment Rules, 2010 correct most but not all of these deficiencies. Paragraph 2(a) of the PML Amendment Rules, 2010 amends Rule 3 to require records “*for all transactions*, including the records of ...cash transactions above INR 1 million, counterfeit transactions and suspicious transactions”. Paragraph 2(b) of the PML Amendment Rules, 2010 amends Rule 4 of the PML Rules to provide that the required transaction records must include “all necessary information specified by the Regulator to permit reconstruction of individual transactions, including the nature of the transaction; the amount and currency in which the transaction was denominated; the transaction date; and the parties to the transaction”. While the PML Amendment Rules cover all transaction records, they do not necessarily require these records to include all of the components required by the FATF standard. While the amended PML Rules may be intended to require all information necessary to permit reconstruction of individual transactions, as written, they require the records to include only “all necessary information *specified by the Regulator* to permit reconstruction of individual transactions” and repeat the components identified before the amendment. Unless the Regulator specifies that transaction records must include account type and identifying number, or clarifies that transaction records must include all necessary information to permit reconstruction of individual transactions, without further qualification, these components would not appear to be required.

506. Rule 9 of the PML Rules elaborates the requirements for customer identification records, specifying in considerable detail the types of identification documents that must be maintained for various categories of customers, including: individuals, companies, partnerships, trusts, and unincorporated associations. However, neither the PMLA nor the PML Rules contain any provisions that require covered institutions to maintain records of account files (other than customer identification documents) and business correspondence. The PML Amendment Rules do not address this deficiency.

507. The Indian authorities have suggested that record-keeping requirements in the Income Tax Act, 1961, as amended, and/or in the Companies Act, as amended, address the transaction and customer identification record-keeping requirements of Recommendation 10. (With respect to transaction records, reliance on these laws is relevant for the period before the PML Rules were amended.) The evaluation team has carefully reviewed these laws and has concluded that they do not satisfy the FATF record-keeping criteria. Section 209 of the Companies Act requires all companies to maintain books of account (including sums received/expended and matters regarding receipt/expensures; sales/purchases, and assets/liabilities) for eight years, but these books of account would not necessarily include customer identification and transaction records that would permit reconstruction of individual customer transactions, as mandated by Recommendation 10. Similarly, the Income Tax Act directs businesses to maintain records sufficient to enable the authorities to determine the businesses’ true income. Here again, the types of records required for this purpose would not necessarily include detailed customer identification and transaction records with the specific information required by Recommendation 10.

508. The Indian authorities have also suggested that sector-specific legislation and regulations, governing banking, securities and insurance, respectively, contain record-keeping requirements that address the requirements of Recommendation 10 for each of these sectors. The evaluation team has carefully reviewed the relevant laws and regulations and, as discussed in greater detail below, has concluded that they appear to address many but certainly not all of the PMLA’s record-keeping gaps, particularly the PMLA’s record-keeping deficiencies for transaction records that existed before the February 2010 amendments.

Institutions supervised by the RBI (except AMCs)

509. It should be noted that there are some restrictions on cash transactions in the banking sector that limited the AML/CFT vulnerability in the banking sector, even before the 2010 amendments required record-keeping for all transactions. The RBI Master Circular requires that remittances of funds by any means (demand draft, mail, or telegraphic transfer) or issuance of travellers' cheques, equal to or above INR 50 000 (USD 1 000), must be conducted by debit to the customer's account or against cheques, and not against cash payment. While this allowed cash deposits up to INR 1 million without triggering record-keeping requirements under the PMLA before the February 2010 amendments, it did, to a limited extent, reduce the AML/CFT vulnerability in the banking sector.

510. Regulations issued under the Banking Regulation Act require banks to maintain certain records that could cover additional types of transactions and include some of the information components missing under the PMLA's record-keeping regime prior to the February 2010 amendments. The Banking Companies (Period of Preservation of Records) Rules, 1985 require banks to preserve, for at least eight years, such records as: all personal ledgers; paid cheques; paying-in slips; vouchers relating to demand deposits, telegraphic transfers, fixed deposits, call deposits, cash credits and other deposit and loan accounts; and account opening forms. The Indian authorities have stated that these records include all customer account records. The Banking Companies Rules also require banks to preserve for five years various bank registers and telegraphic transfer confirmations, and authorise the RBI to direct any banking company to preserve required banking records for a longer period. It appears that these rules would cover most required records for the banking sector, although the Banking Companies Rules do not explicitly require banking companies to maintain records of business correspondence. In addition, there are no requirements in these rules or in any other law or regulation that cover electronic payment records, which represents a significant gap. As a result, it is not clear that the kinds of records specified by the Banking Companies Rules are sufficient to permit reconstruction of individual transactions so as to provide evidence for prosecution of criminal activity. Moreover, these rules do not specify what information the various mandated records must contain, and India has not provided the assessment team an explanation in this regard.³⁷

511. The RBI Master Circular for the banking sector does not constitute law or regulation for the purpose of complying with the requirements of Recommendation 10. The Master Circular does, however, bear on legally binding (OEM) record-keeping requirements and practice in the banking sector, especially before the PML Rules were amended. While the circular does not impose requirements to maintain records for transactions other than those specified in the PML Rules, it does, however, clarify the trigger for the retention period for customer identification records by providing that customer identification records, obtained at account opening and during the course of the business relationship, must be maintained for a period of 10 years "after the business relationship is ended". The circular is silent with respect to maintaining records of account files and business correspondence.

Securities Sector

512. Regulations issued under the Securities Act appear largely to address the pre-February 2010 record-keeping deficiencies identified above. Regulation 17(1) of the SEBI (Stock Brokers and Sub Brokers) Regulations, 1992 requires stockbrokers to maintain an extensive list of books of accounts,

³⁷ The Indian authorities assert that Section 7 of the Information Technology Act, 2000 contains record-keeping requirements that cover electronic payment records. However, that law merely provides that "where any [other] law provides that documents, records or information shall be retained for any specific period, then that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form". The law does not itself require preservation of electronic payment record, and the Indian authorities have identified no other laws or regulations that address this gap.

records and documents that would seem to cover all transactions and customer identification and account files, but not necessarily all business correspondence. The specified records would appear to contain the information components required by Recommendation 10, including the client's account number and type, as well as the other information identified by the FATF standard sufficient to permit reconstruction of individual transactions. Regulation 18 of the SEBI Regulations establishes a five year preservation period for these records, but does not specify the trigger for the retention period. Accordingly, with respect to customer identification and account records, there is no provision in law or regulation that requires such records to be maintained for at least five years following the termination of an account or business relationship. Regulation 38(1) of the SEBI (Depositories and Participants) Regulations, 1996 prescribes a similar five year record-keeping requirements for the records and documents to be maintained by depositories, subject to the same limitations as the stockbroker regulations.

513. In addition, while not “law or regulation” for purposes of complying with Recommendation 10, SEBI has issued legally binding instructions that address intermediaries’ AML/CFT obligations—including record-keeping obligations—in considerable detail that track most of the requirements of Recommendation 10 (SEBI Master Circular). The SEBI Master Circular in effect until 12 February 2010 explicitly requires intermediaries to maintain not only customer identification records, but also account files and business correspondence for ten years. However, the SEBI Master Circular repeats the PMLA Rule’s problematic formulation of the trigger for the retention period, requiring records—including customer identification records—to be maintained for 10 years from the date of “the cessation of transactions” between the client and intermediary. As noted above, this language does not comply with the FATF standard.

514. SEBI issued a new Master Circular on 12 February 2010, consolidating all AML/CFT requirements/instructions issued by SEBI through 31 January 2010. The new Master Circular specifically provides that the records required under the SEBI Act and the PMLA and its Rules³⁸ should be sufficient to permit reconstruction of individual transactions, and specifies that the necessary information includes the amounts and types of currencies involved, if any, as well as the beneficial owner of the account; the volume of funds flowing through the account; and, for selected transactions, the origin of the funds, the form in which the funds were offered or withdrawn (*e.g.*, cheques, demand drafts, etc.), the identity of the person undertaking the transaction, the destination of the funds, and the form of instruction and authority. The new Master Circular also restates the information components required by the PML Rules (transaction’s nature, amount, date, and parties). While it slightly reformulates the trigger for the preservation period—“ten years from the date of transactions between the client and intermediary”—the current wording does not address the concern noted above, with respect to customer identification and account files and business correspondence.

Insurance Sector

515. As a preliminary matter, it should be noted that, to ensure that insurance premiums are paid out of clearly identifiable sources of funds, India limits cash premium payments for all insurance products to INR 50 000 (USD 1 000) (IRDA Master Circular) and requires all premium payments and proposal deposits above that amount to be made by cheque, demand drafts, credit card or other banking channels (IRDA Circular issued on 26 February 2009). This restriction limited the practical impact of the PMLA’s

³⁸ Because it consolidates SEBI’s circulars through 31 January 2010, the new Master Circular continues to identify the transaction records prescribed under Rule 3 of the PML Rules as limited to records of cash transactions greater than INR 100 000; cash transactions with forged or counterfeit currency or bank notes; and all suspicious transactions, whether or not made in cash (par. 6.5). However, the Master Circular also instructs registered intermediaries to ensure compliance with the record-keeping requirements contained in the PMLA and its Rules (par. 6.1). This provision serves to require securities institutions to comply with the record-keeping requirements of the amended PML Rules.

pre-February 2010 threshold of INR 1 million (USD 20 000) for record-keeping for cash transactions, in terms of creating a gap in the record-keeping requirements in the insurance sector.

516. Based on a risk assessment, long-term life insurance products are subject to the PMLA Rule's record-keeping requirements at all stages of the insurance transaction, from initiation to payout (IRDA Master Circular). In addition, IRDA has completely exempted certain categories of insurance products from the PMLA's record-keeping requirements, based on a determination of their very low risk, including group insurance businesses and term life insurance contracts³⁹.

517. While not intended as AML/CFT provisions, the record-keeping requirements of the Insurance Act and its implementing regulations appear to require insurers to maintain records for all transactions, and to require most of the necessary components specified by the FATF standards, including the customer's (and beneficiary's) name, address (or other identifying information normally recorded by the insurance company), the nature and date of the transaction, and the client's account (policy) number and type, which would appear adequate for identification purposes in the insurance context. However, the Insurance Act does not appear to require that transaction records include the type and amount of currency involved. During the on-site visit, insurers stated that they were legally required to retain insurance proposal records, including full documentation that identifies sources of funds and details of bank accounts, based on material completed at the initiation of the proposal, as well as documentation of processing the contract up to the point of maturity. These records would include the insurance policy number and type and are likely to include much of the other information identified as necessary components of transaction records by Recommendation 10. Proposal documentation is mandated in all circumstances under regulation 4(1) of the IRDA Protection of Policy holder Interest Regulations, 2002 which requires that a proposal for grant of a cover, either for life business or for general business, must be evidenced by a written document. The Insurance Act does not set a specific retention period for the required records, but Regulation 25 of the IRDA (Insurance Brokers) Regulations, 2002 requires insurance brokers to maintain all the books of account, statements, documents, etc., for a period of at least 10 years from the end of the year to which they related.

Authorised Money Changers

518. As a preliminary matter, it should be noted that resident Indians can only sell USD 1 000 of foreign currency per transaction, and foreigners and non-resident Indians are allowed to sell no more than USD 3 000 of foreign currency per transaction against payment of cash in INR—with all purchases within a month treated as a single transaction (RBI Circular issued on 27 November 2009). In practical terms, for authorised money changers, this limitation reduces the AML/CFT vulnerability of India's INR 1 million (USD 20 000) threshold for required record-keeping for cash transactions.

519. There appear to be no provisions at the level of law or regulation that directly impose record-keeping obligations on authorised money changers, beyond the requirements of the PML Rules and (for foreign exchange transactions undertaken by banks) the Banking Companies (Period of Preservation of Records) Rules discussed above. The RBI circular for authorised money changers (27 November 2009) merely restates the requirements set forth in the PML Rules and the RBI Master Circular.

³⁹

Exempt insurance products include: stand-alone medical/health insurance products; reinsurance and retrocession contracts, where the contracts are between insurance companies for reallocation of risks within the insurance industry and do not involve transactions with customers; group insurance businesses that are typically issued to a company, financial institution, or association and generally restrict the ability of an individual insured or participant to manipulate its investment; and term life insurance contracts, in view of the absence of cash surrender value and stricter underwriting norms for term policies.

India Post

520. As noted above, was brought under the PMLA in June 2009 by the Prevention of Money Laundering (Amendment) Act, 2009 and accordingly is subject to the record-keeping requirements set out in the PML Rules. In addition, India Post's banking activities ("Small Savings Schemes of the Government of India") are governed by the Government Savings Bank Act, 1873; the Government Savings Certificates Act, 1959; the Public Provident Fund Act, 1968; and various Regulations ("Statutory Rules") issued under each of these Acts. Pursuant to the Statutory Rules, as authorised by the Ministry of Finance - Department of Economic Affairs, the Director General of the Department of Posts has issued procedural rules, including record keeping rules, which are set forth in the Post Office Savings Bank Manuals that are to be considered as legally binding (OEM).⁴⁰ The record keeping requirements established in the Post Office Savings Bank Manuals governed record keeping requirements for the Post Office's banking activities for the period before India Post was covered by the PMLA's record keeping requirements. Under these manuals, customer identification and account records, and most transaction records (including savings bank ledgers, recurring deposit records, cumulative time deposit records) must be kept for a minimum of six years after all the customer's accounts have been closed or transferred, except that signature cards must be kept for at least five years after the account is closed or transferred.

Ensuring records are available to competent authorities on a timely basis

521. Section 12 of the PMLA requires financial institutions to furnish information contained in transaction records to the Director of the FIU within such time as may be prescribed. Section 13 of the PMLA authorises the FIU Director, either of his own motion or on an application made by any authority, officer or person, to call for transaction and customer identification records and make such inquiry or cause such inquiry to be made, as he thinks fit. Section 12 further authorises the Director to impose a fine for failure to comply with the requirement to provide information of between INR 10 000 to INR 100 000 for each failure. The PML Rules specify timeframes for reporting suspicious transactions and large currency transactions, but do not otherwise contain provisions to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority. Indian authorities instruct covered entities to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities, but these instructions are contained only in OEM circulars for the banking, securities, and insurance sectors⁴¹. However, the competent authorities in India have explicit powers in their respective statutes to call for and enforce production of all customer and transaction records and information on a timely basis (e.g., PMLA s.50 (ED and FIU); Banking Regulation Act s.27(2) (RBI); SEBI Act s.11 of (SEBI); and IRDA Act s.14(2)(h) (IRDA)).

Special Recommendation VII

522. In India, scheduled commercial banks, urban co-operative banks, regional rural banks, and State and District level co-operative banks are allowed to conduct domestic wire transfers. The only financial institutions permitted to conduct cross-border wire transfers are banks that qualify as Authorised Persons

⁴⁰ Under the authority of the Director General of Posts, operational postal units are subject to independent audit, including on-site inspections and seizure of records to assess their compliance with all prescribed rules and regulations formulated under various Acts by the controlling Ministry. Non-compliance is subject to sanctions.

⁴¹ In addition, section 27(2) of the Banking Regulation Act, section 11 of SEBI Act, and section 14(2)(h) of IRDA Act authorise RBI, SEBI, and IRDA, respectively, to obtain information from the entities they regulate.

under the FEMA⁴². Domestic money orders have a limit of INR 50 000 (USD 1 000); as noted below, the average domestic money order is INR 1 000 (USD 20). India limits the amount of outbound international wires transfers, depending on the purpose of the transaction, under the FEMA.

523. In addition, India Post, which became subject to the PMLA in June 2009, is authorised to conduct both domestic and cross-border wire transfers. According to the Indian authorities, India Post conducts on average 100 million money orders per year, mostly in small amounts that average INR 1 000 (approximately USD 20). These money orders are primarily from migrant workers to their families. For 2008-2009, domestic money orders constituted more than 99.9% of the total money order business of India Post, in terms of value. Domestic money orders have a maximum limit of INR 50 000 INR (USD 1 000).

524. To conduct international remittances, India Post has a “tie-up” arrangement with Western Union Financial Services Inc, USA (WUFSI) under the Money Transfer Service Scheme (MTSS) to make payments of amounts booked outside India to payees residing in India. This arrangement was approved by the RBI, the Ministry of Finance and the Ministry of Law. Western Union transfers funds to India for India Post by wire through the banking system, using Nostro Accounts in the United States, and collects the charges for remittances into India at the remitters' end, sharing these charges with the India Post. Indian authorities indicate that India Post voluntarily observes RBI guidelines set forth in the RBI MTSS circular dated 7 November 2002 and 27 November 2009, and disseminated these guidelines to all Post offices offering International Money Remittance Transfer Services (IMTS) in 2002 and again in 2009. According to the Indian authorities, India Post voluntarily preserves customer identification and other documents generated at the time of the transaction for 10 years. Similarly, Indian authorities indicate that with respect to international remittances, India Post functions as an agent of Western Union and observes the same limits the RBI prescribes for money transfer operators like Western Union—*i.e.*, for inward remittances, USD 2 500 per transaction, with a maximum of 12 transactions a year. Indian authorities state that, as an agent of Western Union in India, India Post assumes responsibility for the completion of the transaction forms, CDD and record-keeping.

525. In conducting domestic wire transfers, India Post makes payments up to INR 5 000 through Electronic Money Order (eMO) service, delivering the remittance directly to the payee's doorstep, after checking the recipient's identity and address, using a government issued proof of identity. India Post also offers Instant Money Orders (iMOs), whereby it pays the money to the receiver at an iMO Post Office after obtaining the recipient's government issued proof of identity and a secret 16 digit PIN number. Tariffs for domestic products are set by Postal Services Board, Department of Posts.

Obligations on ordering financial institutions to collect and maintain information

526. RBI circulars require full originator information for all cross-border wire transfers--both incoming and outgoing--of any amount. Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, the individual transfers may be exempted from including full originator information, provided that the individual transfers include the originator's account number or a unique reference number and the batch file includes full originator information. Domestic wire transfers of INR 50 000 (equivalent to USD 1 000) and above must also have full originator information, unless this information can be made available to the recipient bank “by other means” (RBI Master Circular and circulars for other RBI-supervised banks)⁴³.

⁴² Full fledged money changers (FFMCs) (remitters/India transfer agents and sub-agents under money transfer service scheme (MTSS) are only permitted to receive inward cross-border money transfer activities under section 10 of FEMA, and are not ordering institutions.

⁴³ For both domestic and cross-border wire transfers, interbank transfers and settlements, where both the originator and the recipient are banks, financial institutions are exempted from originator information

527. RBI circulars explicitly require ordering institutions to verify the originator's identity for all cross-border wire transfers, regardless of the amount. In addition, the 12 November 2009 amendments to the PML Rules require covered institutions to verify identity when carrying out any international money transfer operations, which would include international wire transfers of any amount (Rule 9 (1)(b)(ii) of the PML Rules, as amended). For domestic wire transfers of INR 50 000 (USD 1 000) or above, there is no explicit requirement for ordering institutions to verify the originator's identity, but the November 2009 amendments to the PML Rules obligate covered institutions to verify the customer's identity at the time of opening an account or *executing any transaction equal to or exceeding INR 50 000 (USD 1 000)*, whether conducted as a single transaction or several transactions that appear to be connected. This general CDD provision covers all wire transfers, including domestic wire transfers, of EUR/USD 1 000 or more and satisfies this element of Special Recommendation VII.

528. Legally binding RBI guidance also explicitly requires ordering banks to maintain full originator information for ten years. In addition, intermediary banks must maintain records of all information received from the ordering bank for 10 years when technical limitations prevent full originator information accompanying a cross-border wire transfer from accompanying a related domestic wire transfer. In directing banks to obtain, preserve, and communicate originator information, the RBI guidance emphasises the importance of banks being able to make such information immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets, as well as to the FIU and beneficiary institutions. Under the 10-year record-keeping requirement for all transactions imposed by the 2010 amendments to the PML Rules, it would appear that intermediary institutions, as well as ordering, and recipient institutions, must henceforth maintain wire transaction records for ten years.

Information that must accompany the wire transfer

529. As noted above, India requires originating banks to include complete originator information in the message accompanying all domestic wire transfers of INR 50 000 (USD 1 000) and more, *unless full originator information can be made available to the beneficiary bank by other means*. The RBI Guidelines do not specify what "other means" would permit the ordering financial institution to omit full originator information, but Indian authorities have indicated that "other means" refers to any means that would make full originator information available to the beneficiary bank.

530. During the on-site visit, the Indian authorities expressed the view that the "other means" exemption would apply only (1) where the originator and recipient were the same person or entity and have an account at the recipient institution, so that the receiving bank has complete CDD information on the originator apart from the wire transfer form; or (2) where several individual wire transfers from the same originator are bundled together in a batch file to beneficiaries within India and full originator information is contained in the batch file.

531. For both domestic and cross-border wire transfers, RBI circulars require each intermediary bank in a chain of wire transfers to ensure that all originating information accompanying a wire transfer is retained with the transfer. As noted above, where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the receiving intermediary bank must retain a record of all the information received from the ordering financial institution for at least 10 years.

requirements (RBI Master Circular). This exemption is in accordance with the requirements of Special Recommendation VII, which are not intended to cover financial institution-to-financial institution transfers and settlements where both the originator and the beneficiary are financial institutions acting on their own behalf.

532. RBI circulars require beneficiary banks to implement effective risk-based procedures to identify wire transfers that lack complete originator information. In addition, as an optional matter, the RBI instructions note that the absence of complete originator information “may” be considered as a factor in assessing whether a wire transfer or related transfers are suspicious and whether they should be reported to the FIU as a STR. Beneficiary banks are directed to take up the matter with the ordering bank if a transaction is not accompanied by detailed originator information. If the ordering bank fails to furnish the “detailed information on the remitter,” the RBI guidelines direct the beneficiary bank to consider restricting or even terminating its business relationship with the ordering bank. It should also be noted that there are no time limits on providing originator information for domestic wire transfers in India. During the on-site visit, the assessment team was informed that, by common practice, recipient banks hold wire transfers until they get any missing originator information.

533. Measures are in place for monitoring institutions’ compliance with AML/CFT obligations, including compliance with the requirements of Special Recommendation VII established by the RBI circulars. Sanctions are available in relation to these obligations. In particular, as the relevant regulatory and supervisory authorities, the RBI and the NABARD monitor banks for compliance with the RBI instructions on wire transfers as part of their supervisory inspections. Verification of compliance with the RBI guidelines during supervisory inspections is prescribed in the Department of Banking Supervision’s (DBS) Inspection Manual. Legally binding RBI guidelines on wire transfers have been issued to all financial institutions authorised to conduct wire transfers under the Banking Regulation Act, the PMLA and PML Rules, and the FEMA, and non-compliance is subject to sanctions under section 46(4) of the Banking Regulation Act (see also section 3.10 below).

Additional elements

534. As noted in above, the RBI guidelines require that regardless of the amount, all cross-border wire transfers--both incoming and outgoing--contain full and accurate originator information in the message accompanying the transfer.

Implementation and effectiveness

Recommendation 10

535. India’s record-keeping regime largely complies with the requirements of the FATF standard. The February 2010 Amendments to the PML Rules have corrected most of the previous deficiencies in India’s record-keeping regime. However, it should be noted that the PMLA and the PML Rules as they existed until 12 February 2010, had several gaps in complying with the requirements of Recommendation 10. Until the February 2010 amendments, the PML Rules did not require records for *all* transactions. The PML Rules governing India’s record-keeping requirements during essentially all of the period covered by the mutual evaluation established an INR 1 million (USD 20 000) threshold for cash transaction records, and for non-cash transactions, the PML Rules only required record-keeping for suspicious transactions. These limitations are inconsistent with the express requirements of Recommendation 10 and potentially undermine the availability of transaction records that permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. While sector-specific record-keeping requirements set forth in law or regulation may have addressed most of these gaps, reliance on these general law provisions resulted in fragmented and potentially confusing record-keeping requirements and it is not clear that they require all information components. Although the 12 February 2010 amendments corrected the technical deficiency created by the threshold for cash transaction records, the gap in the record-keeping requirements preceding that date would necessarily have had a significant negative impact on the effective implementation of the record-keeping requirements meeting the FATF standard. Moreover, the gap that existed in the record-keeping requirements before the February 2010 amendments could potentially have an ongoing impact, since relevant records pertaining to transactions not covered by record-keeping requirements before February 2010 may be unavailable.

536. In addition, the PMLA and the corresponding Rules still do not clearly require that the retention period for customer identification records runs from the termination of the account or business relationship, but from the date of the last transaction. This matter is clarified only in OEM, and is not addressed by other general or sector-specific laws or regulations. Also, it should be noted that the effectiveness of customer identification record-keeping may be significantly undermined by problems with the integrity of customer identification documents.

537. Overall, the record-keeping requirements are being implemented effectively. During inspections, examiners review the record-keeping policies and procedures that are in place. India appears to have a strong culture of retaining comprehensive business records for extensive periods. During the on-site visit, the evaluation team was consistently told by both regulators and private sector representatives across all financial sectors that as a matter of common practice, the covered entities retained essentially all business records for an indefinite period.

538. In practice, it may be that even before the recent PML Rules amendments came into force, institutions voluntarily retained transaction and customer identification records that meet the criteria of Recommendation 10. Also, the evaluation team recognises that since cash transactions are prohibited for securities transactions and are limited to INR 50,000 (USD 1,000) for premium payments in the insurance sector, as a practical matter, the PMLA's threshold for required record-keeping for cash transactions was likely to have had somewhat limited impact in these sectors.

539. It should also be noted that before the recent amendments, Rule 5 of the PML Rules directed covered institutions to maintain required records in both hard and soft (electronic) form, in accordance with procedures specified by the sector regulators. (The 2010 amendment to the PML Rules eliminated the requirement to maintain both hard and soft copies of required records.) RBI and SEBI have instructed covered institutions in the banking and securities sectors, respectively, to evolve record preservation systems that allow data to be retrieved easily and quickly whenever required or requested by competent authorities. However, it is not clear whether, and to what extent, the covered institutions in the different banking and insurance sectors in fact keep their records electronically, and whether such records are centralised at headquarters, or are maintained only at the branches⁴⁴. Indian authorities have stated that the information ("elements of data") to be kept in hard/soft copy or at head/branch office would be determined by the scale of operations, nature of business, level of use of technology and organisational policy with regard to maintenance of records. As a result, with respect to the banking and insurance sectors, the assessment team has some concern as to whether, in practice, domestic competent authorities have access to the records and information on a timely basis⁴⁵.

Special Recommendation VII

540. India has established obligations with respect to cross-border wire transfers that appear to largely comply with Special Recommendation VII. India Post is now governed by the PMLA, correcting a significant scope issue that existed before June 2009. Moreover, India Post conducts inward international wire transfers through its tie-up with Western Union, which settles all International Money remittances

⁴⁴ In the securities market, India does not permit "street level account opening"—i.e., brokers cannot execute trades for clients without client details first being uploaded on the master data files of the exchanges, which maintain customer identification records in electronic form. In addition, all transaction records are available with both the stock exchanges and SEBI in electronic mode.

⁴⁵ While the RBI Master Circular instructs commercial banks to monitor accounts using software that provides alerts for potential STRS, this provision does not require centralisation of the alerts. In this regard, the Master Circular provides that "branches not under Core Banking Solution (CBS)" should continue to compile and forward CTRs to the Principal Officer, for transmission to the FIU.

processed by its agents through the banking system. Even before India Post became subject to the PMLA, the use of the banks to affect these cross-border wire transfers reduced their vulnerability to money laundering and terrorist financing, since the banks are subject to obligations with respect to cross-border wire transfers that comply with Special Recommendation VII.

541. With respect to domestic wire transfers, RBI guidelines require full originator information for all domestic wire transfers of INR 50 000 (equivalent to USD 1 000) and above—unless full originator information can be made available to the recipient bank by “other means”. The guidelines do however not specify what “other means” may include.

542. Institutions met with during the on-site visit confirmed that they use the SWIFT system for cross-border transfers, and thus are required by this system to provide certain information as part of their wire transfer instructions. There appears to be positive practice across the financial sector in implementing most of the elements of Special Recommendation VII. The assessment team has however no statistical information with respect to the effectiveness of India Post’s voluntary compliance with RBI wire transfer guidelines.

3.5.2 Recommendations and Comments

Recommendation 10

543. It is recommended that the Indian authorities:

- Bring commodities futures brokers within the scope of the PMLA;
- Amend the PML Rules to require that:
 - the retention period for customer identification records extends at least five years from the termination of the account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).
- Amend the regulatory circulars to remove the total exemption for term life policies from the AML obligations by requiring the maintenance of records of payout transactions (IRDA), including identification of beneficiaries.
- Consider consolidating the regulatory circulars to help ensure consistency of application and avoid unnecessary variations in record-keeping obligations imposed on institutions that are active in the various sectors, and to allow improved group management procedures.

Special Recommendation VII

544. There are no specific recommendations in relation to Recommendation 19.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

| | Rating | Summary of factors relative to s.3.5 underlying overall rating |
|--------|--------|---|
| R.10 | LC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • The requirement that customer identification records need to be maintained for at least five years from the termination of the account or business relationship is not contained in law or regulation. • Sector specific circulars have exempted some insurance products, including term life policies, from AML requirements. |
| SR.VII | LC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ the PMLA did not apply to India Post, which is authorised to conduct both domestic and cross border wire transfers, until June 2009. |

3.6 *Monitoring of transactions and relationships (R.11 & 21)*

3.6.1 *Description and Analysis*

Recommendation 11

545. Rule 2(g) of the PML Rules defines a “suspicious transaction” to include not only a transaction that gives rise to a reasonable ground of suspicion that it may involve the proceeds of a predicate offence, but also a transaction that appears to be made in circumstances of unusual or unjustified complexity, or appears to have no economic rationale or bona fide purpose. The STR reporting obligation meets the requirement to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. Taking into account that the reporting entity will need to decide whether or not to disclose the transactions as suspicious, the requirement to examine as far as possible the background and purpose of such transactions it also met.

546. Moreover, legally binding circulars expressly require all institutions regulated by the RBI; all institutions in the securities sector; authorised money changers; and payment systems operators/gateways to pay special attention to all complex, unusual large transactions and all unusual patterns that have no apparent economic or visible lawful purpose. The extent to which the sector-specific circulars address Recommendation 11’s detailed criteria are addressed below.

Institutions supervised by the RBI (except AMCs)

547. In the banking sector, the RBI Master Circular expressly requires scheduled commercial banks and financial institutions to “pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose”.

548. The RBI circular directs commercial banks to examine, as far as possible, the background and purpose of all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose (including all documents, office records and memoranda pertaining to such transactions); set forth their findings in writing at both branches and the principal officer level; preserve these records for ten years; and make the written findings and related documents available to auditors, the RBI, and other relevant authorities.

549. RBI circulars contain similar requirements for non-commercial banks and non-banking financial companies.

Securities sector

550. The SEBI Master Circular expressly requires securities intermediaries to pay special attention to all complex, unusually large transactions/patterns that appear to have no economic purpose. SEBI imposed additional requirements on intermediaries by a subsequent individual circular, issued on 1 September 2009, that directs intermediaries to examine the background and purpose of all complex, unusually large transactions/patterns that have no apparent or visible economic or lawful purpose--including all documents/office records/memorandums/clarifications sought, pertaining to such transactions--and record their findings in writing. These SEBI instructions further require intermediaries to make the written findings, records and related documents available to auditors and SEBI/stock exchanges/FIU-IND/other relevant Authorities during audits, inspections, or as and when required, and to preserve the records for ten years.

Insurance sector

551. IRDA has issued updated guidance for insurance companies, stating that “It is *advised* that special attention is paid to all complex, unusually large transactions and all unusual patterns which have no

apparent economic or visible lawful purpose and [suspicious] transactions indicated at 3.1.6” (par. 3 (d) – 24 August 2009)). This document further “advises” that the Principal Officer should examine the background of such transactions (but not specifically their purpose) as far as possible, including all relevant documents, office records, and memoranda pertaining to the transactions, “for recording...findings”. On its face, this language would seem to be not mandatory, but merely advice; consequently, it would not qualify as OEM. However, Indian authorities state that in the Indian regulatory context, the term “advise” is synonymous with “direct” and requires compliance. Such an interpretation is supported by the fact that the circular also states that “these records”—evidently meaning the written findings and background documents--“are *required to be preserved* for ten years, as indicated in clause 3.1.10” of the Master Circular. Clause 3.1.10 addresses record-keeping requirements for suspicious transaction reports and reports of counterfeit and high-value cash transactions. As noted above, in India, suspicious transactions include transactions that appear to be made in circumstances of unusual or unjustified complexity, or to have no economic rationale or bona fide purpose. The reference to clause 3.1.10 would thus seem to require insurance companies to keep for ten years documentation for the reports required under Rule 3 of the PML Rules (the STR reporting requirement).

Authorised Money Changers

552. The RBI guidelines for money changers expressly require these institutions to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose, but there are no express requirements to examine the background and purpose of such transactions, set forth their findings in writing, and make the writing findings available to auditors and competent authorities for at least five years (RBI Money Changing Activities Circular (par. 4.6) - (27 November 2009)). Indian authorities point out, however, that the RBI guidance requires the Principal Officer of AMCs to record the reasons for treating any transaction or series of transactions as suspicious—including transactions that are suspicious because they are complex, unusual large transactions, and unusual patterns of transactions that have no apparent or visible economic or lawful purpose—and to make the report available to competent authorities upon request. Since the guidelines require the Principal Officer to file a STR within 7 days of arriving at a conclusion that the transaction is indeed suspicious, it may be that the reference to making “such report” available to the competent authorities upon request refers to the written statement of findings supporting the conclusion, not to the STR itself.

Recommendation 21

Special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations

Institutions supervised by the RBI (except AMCs)

553. There are no express requirements in law, regulation or OEM obligating the banking sector to give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations. In prohibiting correspondent relationships with shell banks, the RBI instructs banks to be “extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and in countries identified as ‘non-co-operative’ in the fight against money laundering and terrorist financing” (RBI Master Circular and similar guidelines for other regulated banks and NBFCs). However, this instruction addresses only one particular type of relationship--correspondent banking. Moreover, it does not directly require banks to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations.

554. Indian authorities state that in circulating FATF Statements concerning the deficiencies in the AML/CFT regimes of certain countries (Iran, Uzbekistan, Pakistan, Turkmenistan and São Tomé and

Principe), the RBI requires (“advises”) banks and financial institutions to take into account the risks arising from these deficiencies. This is relevant, but not sufficient. The FATF standard contemplates that financial institutions must be required to proactively identify jurisdictions that do not or insufficiently apply the FATF recommendations and to give special attention to business relationships and transactions with persons from or in such countries. In identifying such jurisdictions, institutions could rely on publicly available information, such as FATF and FSRB mutual evaluations, proprietary software, and press reporting. The FATF list identifies only a small subset of such jurisdictions. Reliance on it cannot be used to relieve financial institutions of the obligation to identify high-risk jurisdictions and to apply special attention to business relationships and transactions involving such jurisdictions.

555. In terms of indirect requirements, banks and other RBI-regulated entities are obligated to establish and implement their own risk management systems for AML/CTF, including risk-based customer acceptance policies and transaction monitoring. For example, the RBI Master Circular specifically directs commercial banks and financial institutions to establish a risk-based customer acceptance policy that defines risk parameters in terms of the location of the customer and the customer’s clients, as well as such factors as the nature of the business activity, mode of payments, volume of turnover, and customer’s social and financial status. The Master Circular further requires these entities to prepare a profile for all new customers based on risk categorisation, taking into account the above factors, including the location of the customer’s business activity, and to conduct due diligence based on the bank’s risk perception. It could be expected that these systems should include procedures for assessing and paying special attention to the ML and FT risks of customers located in, and transactions from, other countries, including high-risk countries that do not or insufficiently apply the FATF Recommendations. However, such an indirect requirement does not satisfy the requirements of Recommendation 21. Moreover, the RBI guidance appears to focus too narrowly on paying heightened attention to customers from or in high-risk jurisdictions; Recommendation 21 also requires special attention to *transactions* involving such jurisdictions.

Securities Sector

556. The SEBI Master Circular requires securities intermediaries to adopt risk-based CDD, including client acceptance and transaction monitoring, and to pay greater attention to higher risk customer categories. It also explicitly identifies customers in high-risk countries “where the existence/effectiveness of AML/CFT controls is suspect or where there is unusual banking secrecy” as higher risk, requiring enhanced due diligence. In September 2009, SEBI amended the Master Circular to make explicit that high-risk countries include countries that “do not or insufficiently apply FATF standards”. Under the definition of suspicious transaction in Rule 2 of the PML Rules, if transactions involving countries that do not or insufficiently apply the FATF Recommendations have no apparent economic or visible lawful purpose, securities intermediaries are required to examine the background and purpose of such transactions and make written findings available to assist competent authorities and auditors,

Insurance Companies

557. There are no requirements in law, regulation, or OEM requiring insurance companies to give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations. This may be in part because Indian insurance companies are limited in the business they can conduct with persons in foreign countries (see also discussion of Recommendation 22 below).

Measures to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries and counter-measures

558. As noted above, the RBI, SEBI and IRDA have, in some concrete instances, informed the covered institutions about the weaknesses in the AML/CFT systems of other countries, based on FATF

statements publicly identifying such countries, but there has been considerable delay in circulating some of the FATF Statements⁴⁶.

559. With respect to the banking sector, the Indian authorities assert that under section 35-A of the Banking Regulation Act, the RBI has unlimited powers to give directions in the public interest or in the interest of banking policy to all RBI-regulated institutions. In addition, section 11(1) of the FEMA authorises the RBI to direct Authorised Persons with respect to making payments or doing or desisting from doing any other act relating to foreign exchange or foreign securities. However, the RBI does not appear to have exercised its authority to impose counter-measures.

560. The extent to which the Indian authorities can apply appropriate counter-measures in the other financial sectors is unclear. In the securities sector, for example, an amendment dated 1 September 2009 to the SEBI Master Circular directs intermediaries to categorise clients from high-risk jurisdictions, including countries that do not or insufficiently apply FATF standards, as “Clients of Special Category” and to subject such clients “to appropriate counter-measures”. However, the SEBI does not instruct intermediaries to apply specific measures to Special Category Clients. Rather, the guidance states that “appropriate counter-measures” *may* include enhanced scrutiny of transactions relating to non-compliant jurisdictions; enhanced due diligence for business relationships with customers in or from such a jurisdiction; or enhanced or systematic reporting of transactions touching on such countries. In context, this language appears to require intermediaries to apply only enhanced due diligence to high risk customers—not counter-measures to high-risk jurisdictions, as contemplated by the FATF standard. This interpretation is supported by the fact that neither SEBI, nor any of the other Indian regulatory authorities, has exercised specific powers to apply counter-measures by means of enforceable instructions that require financial institutions to apply specific stringent or additional AML/CFT measures, beyond normal obligations set out in their standing circulars (*i.e.*, risk-based scrutiny and internal controls).

561. According to Indian authorities, India can take other counter-measures, such as restricting branches or representative offices of financial institutions from a country that does not have adequate AML/CFT systems or limiting business relationships or financial transactions with identified countries or persons in that country for the banking and financial sector and the insurance sector. As a part of the procedure for permitting entry into India or for considering applications for expanding an existing branch network in India, foreign banks are subjected to various parameters, including the bank’s or its promoters’ country of origin or domicile. Indian authorities report that there have been cases where RBI has not allowed a bank entry into India, due to AML/CFT concerns about the bank’s country of origin or domicile. There have also been cases where a bank has not been permitted to open a branch in India, due to such ML threat considerations. In addition, SEBI considers the country of origin as a primary factor in deciding whether to register a Foreign Institutional Investor (FII)⁴⁷. However, such isolated, individual actions do not necessarily rise to the level of counter-measures. The FATF standard contemplates broader public policy measures, such as adopting an announced policy to restrict branches or representative offices of a specific country, in response to its AML/CFT deficiencies.

⁴⁶ The RBI circulated the FATF Statements of 28 February 2008 and 16 October 2008, highlighting AML/CFT deficiencies in Uzbekistan; Iran; Pakistan; Turkmenistan; Sao Tome and Principe; and the northern part of Cyprus, to commercial banks and financial institutions by circular dated 2 February 2009; the FATF Statement of 25 February 2009 by circular dated 3 June 2009; and the 16 October 2009 FATF Statement by circular dated 20 November 2009. SEBI circulated to stock exchanges and depositories the FATF Statement of 25 February 2009 “for information and appropriate action” on 3 June 2009, and advised them to bring the contents of the FATF Statement to the notice of their members and participants “for information, necessary action and compliance.” In the insurance sector, IRDA circulated the February 2008 FATF Statement on 13 January 2009—almost a year after it was issued.

⁴⁷ To date, no application has been received by SEBI from any FII based in a country that does not have an adequate AML/CFT regime.

Implementation and effectiveness

Recommendation 11

562. It appears that financial institutions rely heavily on software to identify complex, unusual large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose and that in most financial institutions, very large numbers of such transactions are automatically generated. It is unclear whether financial institutions have adequate resources, particularly personnel, to effectively examine the background and purpose of such large numbers of transactions. It is also unclear, given the scale of complex, unusual large transactions or patterns of transactions, whether as a general matter; findings are in fact reduced to writing unless there is a further determination that the transaction is truly suspicious and should be reported to the FIU. Moreover, the fact that so few transactions are identified as suspicious by employees, as opposed to software, raises some questions as to whether front line employees are effectively identifying complex, unusual large transactions, or unusual patterns of transactions and examining their background or purpose, rather than relying on software to flag such transactions.

Recommendation 21

563. Securities intermediaries must give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations, but there are no express, direct requirements in law, regulation or OEM obligating banks and insurance companies, or other financial institutions to give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations.

564. Apart from the problem of delay, when advisories have been circulated regarding the FATF statements, the dissemination mechanism appears to be effective: the banks, intermediaries, and insurance companies with which the assessment team met were familiar with these statements.

565. However, it appears that some Indian officials and financial institutions may be interpreting the requirement to give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations too narrowly. During the on site-visit, some government officials and private sector representatives seemed to limit this obligation to consideration of risks posed by jurisdictions explicitly identified by FATF Statements as insufficiently implementing the FATF standards. Other private sector representatives, however, stated that their institutions employed additional measures to independently identify such high-risk countries, including running proprietary software programs and examining FATF mutual evaluation reports and other publicly available information, and reported that their regulators inspected them to ensure that the institution had established its own, independent system for identifying and giving special attention to relationships and transactions from high-risk jurisdictions. Since many banks, as well as intermediaries and insurance companies, indicated that they had only recently begun to implement their computerised risk-based customer acceptance and transaction monitoring procedures, it is not yet possible to determine whether enhanced CDD is in fact being conducted on business relationships and transactions from or in jurisdictions that do not or insufficiently apply the FATF Recommendations.

3.6.2 Recommendations and Comments

Recommendation 21

566. It is recommended that the Indian authorities:

- Establish clear and direct requirements for the institutions in the banking and insurance sector to pay special attention to both business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations.
- Require all financial institutions to examine the purpose of transactions with persons from or in countries that do not adequately apply the FATF standards in order to determine whether there is an apparent economic or visible lawful purpose. Develop adequate legal authorities to enable it to apply a range of appropriate counter-measures across all financial sectors where a country continues not to apply or insufficiently applies the FATF Recommendations.
- In order to improve the effectiveness of the measures in place, make clear that covered institutions should go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations.

3.6.3 Compliance with Recommendations 11 & 21

| | Rating | Summary of factors relative to s.3.6 underlying overall rating |
|------|--------|--|
| R.11 | LC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • Effectiveness issue: <ul style="list-style-type: none"> ○ Authorised Persons and Payments Service Operators, including India Post, are only covered by the PMLA as of June 2009, making it too soon to assess effectiveness. |
| R.21 | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • There are no clear and direct requirements for the institutions in the banking and insurance sectors to pay special attention to both business relationships and transactions with persons from or in countries that do not, or insufficiently, apply the FATF Recommendations. • Financial institutions are not expressly required to examine the background and purpose of transactions with persons from or in countries that do not adequately apply the FATF standards. • India has no clear legal authority that enables it to apply a range of appropriate counter-measures in the securities or insurance sectors where a country continues not to apply or insufficiently applies the FATF Recommendations. • Effectiveness issue: <ul style="list-style-type: none"> ○ there is a concern that covered institutions do not look beyond the FATF statements, and that they make little use of publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations. |

3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis

567. The reporting obligations of the PMLA and the PML Rules apply to all covered institutions, but not to the commodities futures brokers, which have no reporting obligations. This raises a minor scope issue, which affects the ratings for Recommendations 13 and Special Recommendation IV.

Recommendation 13 and Special Recommendation IV (Suspicious transaction reporting)

568. The PMLA and the PML Rules impose a direct, mandatory obligation, in law and regulation, on all covered entities to report suspicious transactions to the FIU, including attempted transactions,

regardless of the amount of the transaction⁴⁸. As noted above, India defines a “suspicious transaction” to include not only a transaction that gives rise to a reasonable ground of suspicion that it may involve the proceeds of a predicate offence, but also a transaction that appears to be made in circumstances of unusual or unjustified complexity, or appears to have no economic rationale or bona fide purpose. With respect to the proceeds of a predicate offence element of suspicious transactions, the PML Rules were amended on 12 November 2009, to define “suspicious transaction” to include a transaction that “gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offence specified in the Schedule to the Act [PMLA], regardless of the value involved” (par. 2(g) (a)). This amendment corrected a previous limitation in the PML Rule’s STR reporting obligation regarding reporting transactions suspected of involving “the proceeds of crime”. The prior language linked the suspected “proceeds of crime” to the proceeds of PMLA predicate offences and triggered an INR 3 million (USD 60 000) threshold for reporting suspicious transactions involving the proceeds of Part B offences, which only qualify as ML predicates if they generate at least INR 3 million in illicit proceeds. In certain circumstances, this linkage may have unduly restricted the STR reporting obligation: Recommendation 13 requires STR reporting for transactions suspected to involve the proceeds of crime generally (“proceeds of a criminal activity”) without qualification. The impact of the prior limitation may have been significantly reduced by the alternative requirements to report, as suspicious, transactions that appear to be made in circumstances of unusual or unjustified complexity, or to have no economic rationale or bona fide purpose. Nevertheless, as a technical matter, these alternative elements of the suspicious transaction reporting requirement would not necessarily reach all transactions suspected to involve the proceeds of crime generally.

569. The PML Rules require that STRs be submitted “promptly” and not later than seven working days “on being satisfied that the transaction is suspicious”. Reports are required, under the Rules, to be made in writing or by way of fax or e-mail. The FIU indicated that it was generally content with the timeliness of reporting on this basis.

570. The current reporting obligation largely meets the technical requirements of Recommendation 13. It should also be noted that even before the November 2009 Amendment to the PML Rules eliminated the previous threshold on STR reporting for Part B offences, provisions in OEM sought to correct the problem with respect to certain financial institutions. For example, the RBI Master Circular (par. 2.17(b) (iii)), which applies only to commercial banks and RBI-supervised financial institutions, provides that suspicious transactions must be reported “when there is reasonable ground to believe that the transaction involves proceeds of crime generally, irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of the Schedule of the PMLA, 2002”. There are similar provisions for the securities sector (SEBI circular dated 1 September 2009) and for the insurance sector (IRDA circular dated 3 February 2010)—although it should be noted that the insurance sector’s requirement was only imposed after the on-site visit, at the end of the period covered by this mutual evaluation. However, even if these circulars cover reporting transactions involving the proceeds of any crime, including simple theft, the core (asterisked) requirements of Recommendation 13 must be contained in law or regulation in order to be fully met.

571. India imposes in the PMLA and the PML Rules a direct and legally binding obligation on covered institutions to file STRs with respect to transactions that may involve terrorist financing. PMLA Rule 2(g) (as amended, 12 November 2009) requires STRs for transactions that may be linked to the

⁴⁸ Section 12(1)(b) of the PMLA requires covered institutions to furnish information to the FIU on transactions, the nature and value of which may be prescribed. Rules 7(2) and 8 of the PML Rules require covered entities to report to the FIU all suspicious transactions, whether or not made in cash, performed through an extensive--and apparently exhaustive--list of financial transaction mechanisms described in paragraph 3(D).

“financing of activities relating to terrorism”⁴⁹. In addition, under the PMLA, terrorist financing is a Part A (no threshold) predicate offence for money laundering.

572. On its face, the language of the STR reporting requirement, covering transactions relating to the financing of the *activities of terrorism*, requires covered institutions to report suspicious transactions where they suspect or there are reasonable grounds to suspect that the funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations, in compliance with the requirements of both Recommendation 13 and Special Recommendation IV. While the FT offence suffers from some limitations, including whether it covers the sole funding of individual terrorists or terrorist organisations (see section 2.2 above), the STR reporting obligation relating to terrorist financing does not expressly reference the legal definition of terrorism under the UAPA. Both the 12 November 2009 amendment to the PML Rules and the 24 May 2007 amendment, which first expressly included terrorist financing in the reporting requirement, were issued under the PMLA, not the UAPA. However, while the scope of the STR reporting obligation is not by its terms limited by the UAPA definition of terrorism, there is no definition of “activities of terrorism” in the PMLA. Even though the language itself is not expressly limited, this ambiguity leaves it to reporting institutions to interpret the scope of the STR reporting requirement with respect to terrorist financing. To assist reporting institutions, the FIU has provided red flag indicators that help identify financing of activities of terrorism.

Attempted transactions and transactions related to tax matters

573. The 12 November 2009 amendment to the PML Rules requires covered institutions to report suspicious transactions, including attempted transactions, regardless of the amount of the transaction⁵⁰ (section 12(1)(b) of the PMLA and the PML Rules (par. 2(g); see also par. 2(D), 7(2), and 8)). The FIU-IND confirms that it receives STRs regarding attempted transactions. Since tax offences are not ML predicates, the STR reporting requirements apply to transactions relating to tax matters only to the extent that the transaction appears to be of unusual or unjustified complexity, or to have no economic rationale or bona fide purpose. The FIU-IND informed the assessment team that it receives STRs involving tax matters, as indicated in the following table.

STRs Relating to Tax Matters

| Type of Institution | 2006-2007 | 2007-2008 | 2008-2009 | Up to December 2009 | Total |
|-------------------------------|------------|------------|--------------|---------------------|--------------|
| Banks | 105 | 292 | 1 062 | 1 788 | 3 247 |
| Mutual Funds | 113 | 142 | 303 | 208 | 766 |
| Share Brokers/DPs and others | | 13 | 55 | 99 | 167 |
| Insurance Companies | 54 | 113 | 517 | 568 | 1 252 |
| Housing Finance Companies | 18 | 49 | 5 | 3 | 75 |
| Non Banking Finance Companies | 1 | | 8 | 16 | 25 |
| Money Transfer Agents | | 1 | | | 1 |
| Total | 291 | 610 | 1 950 | 2 682 | 5 533 |

Note: The STRs disseminated only to the Central Board of Direct Taxes (CBDT) have been taken as STR relating to tax matters.

⁴⁹ The STR reporting requirement has applied to terrorism/terrorist financing-related transactions since 24 May 2007, when the PML Rules were first amended expressly to include terrorist financing in the reporting requirement.

⁵⁰ While this requirement has only recently been established by law or regulation, as required by Recommendation 13, it should be noted that even before the amendment, the RBI Master Circular for SCBs and financial institutions (par. 2.17(b)(ii)) required banks to report all attempted suspicious transactions, even if not completed by customers. An identical provision for securities intermediaries is set forth in the SEBI Master Circular (par. 10.4).

Additional elements

574. Under the amended PML Rules, financial institutions in India are now required to report to the FIU when they suspect or have reasonable grounds to suspect that the funds are the proceeds of any criminal act committed outside India that would constitute a predicate offence for money laundering domestically, and all or part of the proceeds have been remitted to India.

Recommendation 14 (safe harbour and tipping off)

575. Section 14 of the PMLA provides covered institutions and their officers with protection from civil liability with respect to any reports filed with the FIU. Directors or employees are not expressly covered by the PMLA's safe harbour provision⁵¹. The protection from civil liability is available even if the reporting institution and its officers did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. The PMLA contains no protection from criminal liability with respect to any reports filed with the FIU. However, protection from criminal liability is provided by a provision in the Indian Penal Code (Chapter IV s.76), which specifies that no criminal offence can occur with respect to an act done by a person who is either legally bound to do the act, or who believes in good faith that he/she is legally bound by law to do it. Under this provision, criminal liability does not exist for filing a STR in good faith.

576. The 12 November 2009 Amendment to the PML Rules (par. 7(b)) requires that covered entities and their employees keep the fact of furnishing information on suspicious transactions strictly confidential. As amended, the PML Rules' tipping provision states in relevant part that "a banking company, financial institution or intermediary, as the case may be, and its employees shall keep the fact of furnishing information in respect of transactions referred to in clause (D) of sub-rule (1) of Rule 3 strictly confidential". As formulated in the PML Rules, the tipping off provision is sufficiently broad that it would cover tipping off before, during and after the submission of a STR. The sector regulators have included more detailed provisions prohibiting tipping off in their circulars. Private sector representatives confirmed that they generally did not suspend an account or terminate a customer relationship, once a STR has been filed, but awaited instructions from the FIU, if any. There have been no investigations of alleged tipping off.

Additional elements

577. There are no provisions in the PMLA and the PML Rules, or in binding sector guidelines, that ensure that the FIU keeps confidential the names and personal details of the staff of financial institutions that file a STR. In practice, however, only the name and personal details of the Principal Officer are contained in the STR, and the reporting form contains no reference to the individual staff member who initially identified the suspicious transaction. The FIU-IND states that it does not disclose the details regarding the Principal Officer when it disseminates information to the law enforcement authorities.

Recommendation 25 (only feedback and guidance related to STRs)

578. Section 49(3) of the PMLA provides general authority to the Director of the FIU-IND and other officers to exercise the authorities conferred, and discharge the duties imposed on them under the PMLA, which covers providing feedback to reporting institutions.

579. The FIU-IND and the sector regulators have engaged with reporting entities on STR reporting obligations, with a particular emphasis on reviewing the suspicious transaction identification process and eliminating false positive alerts. According to the FIU, this engagement has increased the reporting

⁵¹ While only the Principal Officers file STRs, the legal responsibility for filing a STR does not rest solely with the principal officer: that individual is simply the avenue through which the communication is made to the FIU.

institutions' awareness of the risks posed by different categories of customers, transactions and products and has resulted in reporting entities' fine-tuning their alert generation and suspicious transaction review systems. The FIU also states that the quality of STRs submitted by the reporting entities has improved substantially, due to feedback on STRs and the institutions' active involvement in the FIU review process.

580. Indian authorities use several mechanisms to provide guidance and both general and specific (case-by-case) feedback related to STRs and STR reporting:

581. **Feedback on receipt of report:** FIU-IND provides confirmation and a unique acknowledgement number to reporting entities on receipt of each STR that is used in future interactions with the FIU. If, in analysing a particular STR, the FIU finds that the information provided is insufficient, the FIU returns the STR to the reporting institution with instructions to correct the deficiencies.

582. In addition, since 2008, the FIU has used a "compliance module" for STRs that identifies certain information about the quality of a reporting institution's STRs, including the number of instances in which the FIU has returned an inadequate STR for additional information. The module helps FIU-IND monitor compliance with PMLA reporting obligations by particular institutions, and provides a basis for detailed feedback.

583. **Outreach Meetings:** The FIU-IND conducts numerous sector-specific outreach and training meetings for reporting institutions--including seminars, conferences and workshops--to provide information on AML/CFT requirements, including STR reporting, and on ML techniques, trends and patterns. These meetings generally address a broad range of AML/CFT obligations, not just STR issues. In the STR part of the curriculum, they often provide general feedback on the information and insights gained from STRs received by the FIU, including sanitised cases and presentations on the types of suspicious transactions reported. This material is intended to help financial institutions better understand risk indicators and improve their systems for identifying and reviewing suspicious transactions. In this regard, the FIU provides current ML "scenarios", based on current AML/CFT trends and techniques identified through STRs and other means, as part of a continuing effort to help reporting entities implement internal "Alert Management System Review" mechanisms that update and adjust the parameters of their automatic suspicious transactions alert systems. Many of the FIU's outreach events are aimed at training professional trainers to conduct AML/CFT training programs in their respective institutions to increase employee and management awareness of ML/FT issues.

584. **Focused Sector-Specific STR Review Meetings:** The FIU-IND also conducts periodic sector-specific STR review meetings to provide feedback on suspicious transaction techniques and trends (based on STRs), and to offer detailed guidance for improving the quality of the STRs. These review meetings are attended by reporting entities, regulators, and sector associations. As in the broader AML/CFT outreach meetings, the STR review meetings in part seek to provide information on current ML scenarios to help reporting entities refine the parameters of their automatic suspicious transactions alert systems. According to the FIU, during the STR review meetings, it provides statistics on the number of STRs submitted by the sector's reporting entities; analyses the quality of sample STRs to identify shortcomings and possible areas of improvement; explains the types of reporting information that would be useful to the FIU and law enforcement authorities; and compares the performance of reporting entities within and across the different sectors. In addition, examples of sanitised cases and feedback from the law enforcement authorities received by the FIU are shared and discussed, and reporting entities are provided an opportunity to give presentations on their AML/CFT systems and share relevant experiences.

585. **Individual STR Review Meetings:** The FIU also holds periodic individual review meetings with the Principal Officers of the most important reporting entities, to review the performance of individual reporting entities. During these meetings, the FIU provides concrete feedback on the quality of the

institution's STRs, the types of information that should be included in STRs to make them more useful to the FIU and law enforcement, and steps the reporting entity should take to improve the effectiveness of its suspicious transaction identification and reporting system. Statistics regarding outreach and review meetings are provided in the following table:

| | 2006-2007 | 2007-2008 | 2008-2009 | Up to Dec 2009 | Total |
|---|-----------|-----------|-----------|----------------|--------|
| Number of Seminars and Training Workshops | 57 | 93 | 103 | 60 | 313 |
| Number of participants in Seminars/Workshops | 2 749 | 5 479 | 3 617 | 2,657 | 14 502 |
| Number of review meetings with Principal Officers | 6 | 12 | 14 | 21 | 53 |
| Number of participants in review meetings | 216 | 379 | 335 | 370 | 1 300 |

586. **FIU-IND Annual Report:** The FIU provides statistical feedback on STR reporting that includes breakdowns by sector; the nature of suspicion (e.g. false identification documents, unverified address, large number of accounts, known criminal associations, unusual account activity, structuring, questionable source of funds); and dissemination. The Annual Report of the FIU-IND also contains indicators for different types of suspicious transactions.

587. **Web portal for reporting entities:** The FIU-IND website also provides reporting entities with sector-specific guidance on STR reporting, including respective indicators of suspicious transactions for banking, securities, and insurance companies, as well as answers to frequently asked questions on reporting procedures and formats.

Recommendation 19 (Other reporting)

588. Section 12(1)(b) of the PMLA and Rule 3(1)(A) and (B) and Rule 8 of the PML Rules require covered institutions to report to the FIU all cash transactions greater than INR 1 million (USD 20 000) or its equivalent in foreign currency, including all series of integrally connected cash transactions occurring within a month that together exceed the INR 1 million threshold. Currency transaction reports (CTRs) must be filed on a monthly basis (PMLA Rule 8). RBI, SEBI and IRDA circulars provide instructions on the procedure and manner of furnishing CTRs to the FIU. Although both the manual and electronic reporting is permitted by regulation, the FIU has directed reporting entities to adopt electronic CTR filing on an expedited basis and has provided a Report Preparation Utility (RPU) to the reporting entities to help them generate reports in electronic format. Electronic CTR filing reached 99.84% in 2008-2009.

589. The table below gives an overview of the number of CTRs from the reporting entities since it became operational in March 2006:

Receipt of Cash Transaction Reports (CTRs)

| Subcategory | 2006-2007 | 2007-2008 | 2008-2009 | Up to Dec 2009 | Total |
|------------------------------|------------------|------------------|------------------|------------------|-------------------|
| Public Sector Banks | 921 597 | 2 062 742 | 3 108 675 | 3 153 079 | 9 246 093 |
| Indian Private Banks | 1 133 138 | 1 654 749 | 1 980 045 | 1 382 095 | 6 150 027 |
| Private Foreign Banks | 60 504 | 84 407 | 88 239 | 63 927 | 297 077 |
| Others | 25 529 | 158 015 | 334 191 | 295 587 | 813 322 |
| Total | 2 140 768 | 3 959 913 | 5 511 150 | 4 894 688 | 16 506 519 |
| Manual CTR | 81 368 | 15 470 | 9 001 | 2 279 | 108 118 |
| % Electronic receipt of CTRs | 96.20% | 99.61% | 99.84% | 99.95% | 99.34% |

Additional elements

590. Information provided by the CTRs is filed in the electronic database maintained by the FIU-IND. This database is searchable on various parameters, allowing the FIU to mine data linking persons/accounts/transactions filed therein. The FIU uses the CTR database to help analyse STRs, process requests for information from competent authorities, and generate clusters of CTRs that, e.g., help identify possibly related clusters of high-risk customers and geographic locations. This information and analysis is made available to law enforcement and other competent authorities⁵². The CTR database is protected in the same way as the other information in the possession of the FIU (see section 2.5 for more details).

Implementation and effectiveness

591. India's STR reporting requirements have been in effect since the PMLA came into effect in July 2005 and the reporting obligation specifically included terrorist financing beginning in 2007. The FIU has been operational and receiving STRs since March 2006. The country has made important progress in establishing its STR reporting regime since that time, and the total number of STRs has been rising—from 817 in 2006-2007, to 4 409 for 2008-2009, 5 856 on 31 December 2009, and 8286 as of 12 February 2010, at the end of the period covered by the mutual evaluation⁵³. The FIU reports that for 2009-2010 (as of 31 December 2009) it had received 225 STRs relating to attempted transactions. As the table below reflects, for 2008, there was a particularly high level of STR reporting by foreign private banks, compared to private Indian banks. This trend was reversed the following year and the Indian authorities explained that was because Indian banks improved their capacity and technology.

Number of STRs submitted by different subcategories of reporting entities

| | 2006-2007 | 2007-2008 | 2008-2009 | Up to Dec 2009 | Total |
|-----------------------|-----------|-----------|-----------|----------------|--------------|
| Banks | | | | | |
| Private Indian Banks | 234 | 677 | 871 | 1 456 | 3 238 |
| Private Foreign Banks | 184 | 386 | 1078 | 606 | 2 254 |

⁵²

The FIU is currently analysing CTRs relating to high risk businesses and threshold values, and the resulting report will also be made available to competent authorities.

| | 2006-2007 | 2007-2008 | 2008-2009 | Up to Dec 2009 | Total |
|---|------------|--------------|--------------|----------------|---------------|
| Public Sector Banks | 15 | 91 | 429 | 621 | 1 156 |
| SBI and its Associates | 1 | 14 | 436 | 1 339 | 1 790 |
| Co-operative Banks | 3 | 15 | 12 | 26 | 56 |
| Total | 437 | 1 183 | 2 826 | 4 048 | 8 494 |
| Financial Institutions | | | | | |
| Insurance Companies | 57 | 182 | 668 | 648 | 1 555 |
| Housing Finance Companies | 21 | 55 | 61 | 17 | 154 |
| Non Banking Financial Companies | 3 | 1 | 11 | 27 | 42 |
| Money Transfer Service Agents and Others | 7 | 50 | 101 | 297 | 455 |
| Total | 88 | 288 | 841 | 989 | 2 206 |
| Intermediaries | | | | | |
| Mutual Fund | 218 | 392 | 624 | 539 | 1 773 |
| Share Brokers, Depository Participants and Others | 74 | 53 | 118 | 280 | 525 |
| Total | 292 | 445 | 742 | 819 | 2 298 |
| Grand Total | 817 | 1 916 | 4 409 | 5 856 | 12 998 |

592. Based on the figures in the table below, the reporting within each of the different components of the financial sector (banking, securities, and insurance) is evenly spread. Reporting by the top five entities in terms of market share is more or less equivalent with their market share. In the banking sector, 41 percent of STRs are submitted by five banks that have 38 percent of the market share; in the securities sector, one third of STRs are filed by five mutual fund entities that have 57 percent of the market share; and in the insurance sector, 60 percent of STRs are submitted by five life insurance companies that have 84 percent of the market share. In the securities sector, 28 percent of STRs are submitted by the top five stock brokers and depositories, which have a 36 percent market share.

STRs submitted by major reporting entities (by market share)

| Sector | Basis for computation of market share | Percentage market share of top 5 reporting entities in the sector | Percentage share of STRs submitted by the top 5 reporting entities in the sector |
|---------------------------------------|--|---|--|
| Banking | Deposits as on March 2009 | ~38% | ~41% |
| Life Insurance Companies | New Business premium received in 2009 | ~84% | ~62% |
| Housing Finance Companies | Outstanding loans as on March 2009 | ~84% | ~52% |
| Mutual Funds | Assets under management (October 2009) | ~57% | ~33% |
| Share Brokers/Depository Participants | Number of Active Clients | ~36% | ~28% |

593. India has established a system where each reporting entity must designate a single Principal Officer, whose responsibilities include making a final institutional determination on whether a transaction is suspicious for filing purposes, and filing any resulting STRs with the FIU. There are 13 000 such officers nationwide. The FIU and sector regulators have encouraged reporting entities to adopt AML software to generate alerts on scenarios relevant to the products and services offered by them, and have

provided training and guidance on identifying suspicious transactions (see discussion of Recommendation 25 above). During the on-site visit, both government officials and private sector representatives told the assessment team that most reporting entities in their sectors have incorporated indicators, based on risk of products/services offered, customer and transaction type, to help identify suspicious transactions. According to FIU officials, approximately 75% of the STRs are based on alerts generated automatically from centralised software, with the remainder initially identified as potentially suspicious by human assessment. According to Indian officials, many of the scenarios used to identify potentially suspicious transactions involve consideration of multiple transactions, rather than single transactions, and require preliminary analysis by the reporting entity to determine whether there is a basis for actual suspicion. The level of analysis that reporting institutions are expected to perform appears consistent with that in most STR systems, which make it the responsibility of the institution to satisfy itself that there are genuine grounds for suspicion before filing. Indian officials consistently stated that the Principal Officer is not supposed to investigate transactions beyond establishing reasonable grounds for suspicion, and is not responsible for building a case.

594. The FIU and sector regulators have encouraged reporting entities to file STRs with the FIU electronically. The FIU-IND provides report preparation utilities to help reporting entities prepare and submit the prescribed reports in electronic form, and, as indicated before, more than 99% of the STRs received by the FIU-IND are in electronic form. In addition, the RBI has encouraged banks to implement the Core Banking Solution (CBS), a centralised banking system internally connecting all bank branches to headquarters, which allows all data—including information relevant for identifying and filing STRs—to be available at bank headquarters.

595. The regulators' supervisory inspections include review of reporting functions and compliance; FIU-IND helps train the examiners in this area. In addition, the FIU conducts occasional targeted inspections when it needs to verify specific compliance related issues. In 2009, the FIU conducted one such targeted inspection, resulting in issuance of a show cause order to the bank.

596. Despite the positive efforts of officials and reporting entities, as well as the threat of sanctions for failing to report, the reporting of STRs (especially in the banking sector) appears to be extremely low, both in terms of absolute numbers and in comparison with the size of the country and its economy. India has a population of approximately 1.17 billion (as of July 2009), making it the second most populous country in the world. There are over 82 000 commercial bank branches throughout India— among the largest number of banks in a country in the world. There are also (as of 31 March 2009) 9 622 registered stockbrokers, 62 761 registered sub-brokers, and 44 insurers/reinsurers. And there are approximately two-to-three million proceeds-generating offences a year in India, including more than 82 000 economic crimes. Yet, as the statistics (table with the number of STRs submitted by different subcategories of reporting entities) show, in 2008-2009, a total of 4 409 STRs were filed across all sectors. In 2009-2010, that number increased, to 5856 STRs on 31 December 2009 and 8286 as of 12 February 2010, but this is still very low, given the scale of India's financial sector. According to the FIU, it currently receives about 50 STRs a day, in a country where there are approximately 5.5 million banking transactions per day. The banking sector in particular is large, important and growing. Yet the number of STRs in the banking sector is strikingly low—2 826 STRs filed by banks in 2008-2009 and 4 048 STRs filed by banks in 2009-2010 (to December 2009).

597. The low rate of STR reporting raised significant concerns for the assessment team about the effectiveness of India's implementation of its STR reporting regime. In seeking to address this issue, however, the assessment team necessarily recognised that there are no generally accepted benchmarks or an established analytic basis for determining whether the level of STR reporting in a given country is

appropriate and reflects an effective reporting system⁵⁴. In addition, in evaluating compliance with Recommendation 13, the evaluation team was aware that an over-emphasis on the number of STRs filed could have an unintended and deleterious effect of encouraging officials to implement reporting regimes aimed at generating a “required” quantity of reports, instead of focusing efforts on obtaining genuinely useful, high-quality STRs. The assessment team was therefore sensitive to the need to avoid adopting an arbitrary level of suspicious transaction reporting as a de facto benchmark for assessing compliance with the requirements of the FATF standards in the context of a particular financial system. This is especially the case where, as here, the STR reporting system is only a few years old and reporting is solidly trending in a positive direction, with active engagement by both reporting entities and the FIU. In this regard, it should be noted that STR reporting more than doubled each year between 2005-2006 and 2008-2009, and, as of the end of the period covered by the mutual evaluation, was on track to do so for 2009-2010 as well.⁵⁵ In addition, Indian officials emphasise that they closely monitor STR reporting patterns and practices in an ongoing effort to ensure robust and appropriate reporting, in light of AML/CFT risks, and that they are committed to continuing to work with reporting entities across the financial sector to improve STR reporting.

598. Indian officials have offered a variety of explanations for the country’s low reporting rates. During the on-site visit, FIU officials stated that the FIU-IND works closely with the banking sector to help ensure that “false alerts” are filtered out and only “real” STRs are filed. According to the FIU, Principal Officers filter out about 90 % of the internal alerts on potentially suspicious transactions before filing STRs, although the bankers themselves estimated that less than 2% of the alerts would result in reports being filed with the FIU-IND. According to the FIU, during the review process, the reporting entities link alerts related to the same person or related persons and examine them in the context of the customer’s profile. Certain alerts are closed because the nature of the customer’s business or other related information adequately explains the alert. Grouped alerts that are not closed are submitted as STRs. According to the FIU-IND, on an average, one STR covers approximately 38 transactions, however, it is not clear whether these additional transactions are individually suspicious, or whether they merely represent related transactions that the reporting institution felt would assist the analysis of the actual suspicious transaction. Indian authorities and numerous private sector representatives also asserted that the apparently low number of STRs merely reflects the removal of low quality, “useless” alerts before filing. The FIU-IND indicated that it actively engaged with the institutions to discourage defensive reporting and to improve the overall quality of STRs. According to Indian officials, reporting entities’ engagement in reviewing alerts has improved their awareness of the risks posed by different types of customers, transactions and products, resulting in reporting institutions fine-tuning their alert generation and review systems and substantial improvement in the quality of submitted STRs. Part of this process involves encouraging institutions to think more specifically about the potential origin of the funds (*i.e.* the likely

⁵⁴ According to the mutual evaluation report of Germany, the IMF has attempted to normalize reporting levels against population, as well as against GDP. The results suggest that most countries assessed LC or higher for Recommendation 13 receive in the range of 40–200 STRs per 100,000 of population. However, the assumption that the amount of money laundering activity in an economy is linked to the size of its population appears questionable. Population alone does not generally drive economic output—and the criminal economy and money laundering activity are economic outputs. The problem of benchmarks is exacerbated in a developing country like India, where a large part of the population does not participate in the financial system. In a context where lack of financial inclusion is a significant problem, it does not seem appropriate to compare the number of STRs/ per 100,000 of population. Apart from these obstacles, it would be challenging to identify relevant countries for comparison.

⁵⁵ India reports that there were 10 067 STRs across all sectors for the entire 2009-2010 financial year (ending 31 March 2010). This figure covers a period that goes significantly beyond the 12 February cut-off date for the mutual evaluation, and is noted here only for purposes of showing the steady increase in STR reporting levels.

predicate offence) rather than reporting on the basis of a mere suspicion. It is possible that, in response to this, institutions are taking an overly cautious approach to reporting, thereby denying the FIU important intelligence.

599. In addition, Indian officials sought to explain the relatively low STR reporting rate by reference to the banking system's large numbers of low-risk/low-value customers, which are estimated by the banks to account for about 90 % of their clientele, and the small average value of transactions⁵⁶. The size of the low-risk/low-value customer base generates fewer suspicious transactions, according to Indian officials. While this may be true, India nevertheless has a very large financial system, both in terms of assets and the numbers of bank branches, transactions, and customers. The financial sector is certainly not without high-value, high-risk customers and transactions. Both Indian authorities and private sector representatives also explained that many reporting entities have only recently implemented software systems to generate automatic suspicious transaction alerts, which are estimated by the banks to produce the basis for 60%-80% of their STRs. As these systems increasingly come into operation, and as financial institutions gain experience and become increasingly sophisticated in identifying suspicious transactions, Indian officials expect that the number of STRs will continue to increase significantly. While lack of experience and sophistication with respect to STR reporting may help explain the current low numbers of STRs, it suggests that although improving, implementation to date has been less than robust, given that the PMLA's reporting requirements came into force 1 July 2005.

600. Another possible contributor to the low number of reports could be the interface between CTRs and STRs. (FIU-IND receives approximately 600 000 CTRs, containing around 8 million transactions, every month.) In some discussions with the private sector, there were suggestions that, if a CTR were filed, the transaction would not be reviewed further to determine whether it might also be suspicious, unless there were concerns that it might be part of a tiering or "smurfing" operation, or where the cash transactions are not consistent with the customer profile. However, Indian authorities informed the assessment team that approximately 20% of STRs in the banking sector contain transactions that were also reported as CTRs.

601. Overall, the evaluation team was unable to develop a clear explanation of India's apparently low number of STRs (taking the number at face value, rather than the number of transactions covered), and the issue remains of concern. While India's STR reporting requirements now satisfy the technical elements of the FATF standard, the low STR reporting rate--including the disproportionately low rate in the banking sector, compared to securities and insurance sectors--raised serious questions as to effectiveness and caused the evaluation team considerable difficulty in determining the appropriate rating for Recommendation 13. The evaluation team recognises the technical compliance of India's STR reporting regime, as well as the steady upward trending of the reporting levels, and the lack of accepted numerical benchmarks for measuring effectiveness. In particular, the team reiterates that its concern regarding the effectiveness of India's STR reporting regime should not be misinterpreted as based on low numbers alone, but is based on a number of factors, identified above and listed as deficiencies in the Recommendation 13 ratings box. Given the importance of this issue, it is strongly recommended that the Indian authorities thoroughly examine the STR reporting rates and seek to determine whether the number of overall STRs is

⁵⁶ India's per capita Net National Product (at constant prices) is approximately INR ~25 494 (USD 505) (2008-2009). Most financial transactions that would potentially generate STRs are small, reducing the ML (but not TF) risk: domestic money orders average approximately INR 895 (USD 18); NEFT remittances average of approximately INR 53 000 (USD 1 060); the average balance in post office savings accounts is approximately INR 3 000 (USD 60); the average balance in post office recurring deposit accounts is approximately INR 9 000 (USD 180); the average deposit/bank account is approximately INR 56 000 (USD 1 120). Similarly, Indian authorities point out that while there are 82 000 commercial bank branches in the country, 63% of them are in rural/semi-urban areas with low/value customers/transactions that involve relatively few suspicious transactions.

adequate, given the size of the financial sector and the number of proceeds-generating crimes; whether specific sectors are not reporting appropriate numbers of STRs; if STR reporting levels are inadequate, either overall or by specific sector, the reasons for such low reporting and appropriate responses to correct the underlying problems; and the understanding of reporting entities of the evidentiary standards for filing STRs, including the level of pre-filing analysis and investigation considered necessary to make a filing decision. Such information could include the information the reporting entities collect to file a typical STR and whether reporting entities believe they should, or do (sometimes/often) conduct medium or long term monitoring of accounts to help determine whether a transaction is truly suspicious for filing purposes.

602. In addition, given India's vulnerability to terrorism and the large number of actual terrorist attacks per year⁵⁷, the number of terrorist related STRs also appears to be extremely low, raising further questions about the implementation and effectiveness of the STR reporting obligation. Between 2006 and December 2009, the FIU-IND received 203 STRs explicitly identified as terrorist-related by the reporting entity. Another 105 STRs filed by banks April 2009 through February 2010 were terrorism-related but were not explicitly identified as such by the reporting entity, and instead were identified as terrorism-related by the FIU's analysis⁵⁸.

603. Moreover, as the chart below shows, through 2008, almost all STRs explicitly identified as terrorism related by the reporting entities were identified based on a match with names on terrorist designation lists. The failure of front line employees in reporting institutions to identify FT-related STRs by means other than automated matching alerts further suggests that there may be problems in effectively implementing this important component of the STR reporting obligation. Since terrorist financing transactions typically involve relatively small amounts, dispersed to a variety of groups, individuals, and/or regions, and do not necessarily involve criminal proceeds, terrorist financing transactions may not trigger automated alerts. It is all the more important, therefore, for the financial institutions in India to implement STR identification and reporting procedures that effectively make use of trained human judgment on the front lines of financial transactions.

STRs explicitly identified as FT-related

| | 2006-2007 | 2007-2008 | 2008-2009 | 2009-2010 (up to December 2009) |
|---|-----------|------------|-----------|------------------------------------|
| STRs identified on the basis of a match with FT related lists | 40* | 117* | 6 | 8 |
| STRs explicitly identified as FT-related by ways other than a match with FT related lists | 4 | 16 | 8 | 4 |
| Total STRs on FT | 44 | 133 | 14 | 12 |

⁵⁷ Indian authorities estimate that expenditures for terrorism directed against India total approximately USD 30-40 million per year, but that about 70 % of these funds go to infrastructure for terrorism outside India, including infrastructure for terrorist organisations' headquarters; field infrastructures, supply lines, training camps, communication centres, weapons, explosives and other procurements and also towards salaries/subsistence to the terrorists and their families. The 30 % of terrorist financing estimated to occur within India itself relates primarily to funds for special operations and subsistence maintenance of terrorists and their families.

⁵⁸ India's STR reporting format does not contain a separate text box for capturing information on whether the report is explicitly terrorism-related, and most reporting entities do not clearly classify the STR as FT related by explicitly mentioning 'terrorist financing' as the grounds of suspicion, even when the STR has been generated because it involves a typical FT scenario. However, some STRs are subsequently identified as terrorism related by the FIU review of the fact pattern discussed in the grounds of suspicion. The FIU-IND classifies terrorist funding STRs identified by the FIU analysis in a separate category than STRs identified as terrorism-related by the reporting entity.

604. After MSBs were brought under the PMLA regime in June 2009, the FIU-IND provided this category of reporting entities with scenarios involving medium to high FT risk (e.g., multiple transfers from different individuals/entities to one individual/entity, and/or involving high-risk geographic areas).and mandated automatic reporting based on these parameters. While this system has generated a very large number of automatic terrorist-related transaction filings from MSBs, the FIU-IND does not categorise them as STRs because the transactions are not reviewed by the reporting entities and found to be genuinely suspicious before submission. This approach seems reasonable.

605. Indian authorities seek to explain the strikingly low number of terrorist-related STRs on the grounds that only a very small percentage of the terrorist funding is routed through the formal financial sector and such transactions are notoriously difficult to identify. This may be true, but given the scale of India's formal financial sector and the high level of terrorist activity and related FT risk in the country, the extremely low level of TF STRs from banks, in particular, raises grave concern that reporting institutions are not identifying TF-related suspicious transactions.

606. Whatever sensitivities to benchmarks are appropriate, given the high risk of terrorism and terrorist financing in India, the evaluation team is convinced that the number of STRs received by the FIU-IND is simply too low and reflects a serious shortcoming with respect to effectiveness.

3.7.2 Recommendations and Comments

Recommendation 13 and Special Recommendation IV

607. It is recommended that the Indian authorities:

- Thoroughly examine the STR reporting rate, to determine whether it is adequate, given the size of the financial sector and the number of proceeds-generating crimes; whether specific sectors or geographic regions are not reporting appropriate numbers of STRs; and, if STR reporting levels are inadequate, either overall or by specific sector/area of the country, the reasons for such low reporting and appropriate responses to correct the underlying problems. Particular attention should be paid to the disproportionate reporting levels between the banking sector and the securities and insurance sectors.
- Thoroughly examine the STR reporting rate with respect to terrorism-financing related STRs in particular, to determine why the number of such STRs appears to be extremely low, both in terms of the size of the financial system and relative to the terrorist financing risk, and why so few of the FT-related STRs have been identified by means other than automated alerts triggered by matching names to terrorist lists, and take appropriate steps to correct any underlying problems.
- Conduct intensive outreach, focusing on MSBs and banks, to improve capacity to identify and report TF-related suspicious transactions.
- Clarify the scope of the language of the STR reporting requirement covering transactions relating to the financing of the *activities of terrorism* to ensure that it requires covered institutions to report suspicious transactions where they suspect or there is reasonable grounds to suspect that the funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations,

Recommendation 14

608. Expand the PMLA's safe harbour provision to expressly cover directors or employees.

Recommendation 19

609. There are no specific recommendations in relation to Recommendation 19.

Recommendation 25

610. There are no specific recommendations in relation to Recommendation 25.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

| | Rating | Summary of factors relative to s.3.7 underlying overall rating |
|--------------|---------------|---|
| R.13 | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. ○ there is no definition of “activities of terrorism” in the PMLA, leaving it to reporting institutions to interpret the scope of the STR reporting requirement with respect to the financing of the activities of terrorism. • Effectiveness issues: <ul style="list-style-type: none"> ○ concerns about the low number of STRs filed in relation to ML and FT (especially in relation to the banking sector). ○ |
| R.14 | LC | <ul style="list-style-type: none"> • Directors or employees are not expressly covered by the PMLA’s safe harbour provision. |
| R.19 | C | This Recommendation is fully observed. |
| R.25 | LC | <i>(This is a composite rating and does not derive from the issues covered here.)</i> |
| SR.IV | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. ○ There is no definition of “activities of terrorism” in the PMLA, leaving it to reporting institutions to interpret the scope of the STR reporting requirement with respect to the financing of the activities of terrorism. • Effectiveness issues: <ul style="list-style-type: none"> ○ concerns about the extremely low number of STRs filed in relation to FT in comparison with India’s vulnerability with regard to terrorism. ○ |

3.8 Internal controls, compliance, audit and foreign Branches (R.15 & 22)

3.8.1 Description and Analysis

Recommendation 15

All institutions covered by PMLA

611. The PMLA contains no requirements with respect to internal procedures, policies and controls to prevent money laundering and terrorist financing, but the PML Rules require covered entities to: develop an internal mechanism for maintaining required records (PML Rule 5(2)); implement a client identification program (PML Rule 9(7)); and designate a “Principal Officer,” responsible for furnishing required information—including STRs-- to the FIU (PML Rule 7(1)). The PML Rules are silent on the need for a co-ordinated AML/CFT program, independent audit procedures, and structured staff training. Rule 7(3) provides only that “institutions *may* evolve an internal mechanism for furnishing information in such form and at such intervals as may be directed by the regulatory authorities.” Moreover, the role specified in the PML Rules for the Principal Officer is far narrower than a money-laundering compliance officer and relates only to the transmission of reports to the FIU, not to overall compliance, and there is no requirement that the principal reporting officer be a management level position. However, the RBI, SEBI

and IRDA have issued supplementary instructions under the PML Rules, establishing requirements for internal AML/CFT procedures, policies and controls for their respective sectors, as discussed below.

Internal Policies, Procedures and Controls

Banking sector (including AMCs)

612. In addition to re-stating the PMLA's requirements for internal policies and procedures that cover record retention, CDD, and the Principal Officer/reporting obligation, the RBI Master Circular requires that a covered institution's Board of Directors must ensure that an effective KYC program is put in place by establishing appropriate policies and procedures and ensuring their effective implementation. These must include: customer acceptance policy; customer identification procedures; transaction monitoring; risk management; proper management oversight, systems and controls; segregation of duties; training and other related matters. Responsibility for ensuring that the bank's policies and procedures are effectively implemented must be explicitly allocated within the bank. In addition, banks, in consultation with their Boards, are explicitly required to devise procedures for creating risk profiles of existing and new customers and to apply risk-based AML measures, based on the risks involved in a transaction, account or banking/business relationship (monitoring and detection of unusual and suspicious transactions).

613. RBI circulars require banks and other RBI-supervised financial institutions to designate a senior management officer as the Principal Officer, to be located at the bank's head/corporate office. The Principal Officer is expressly responsible for transaction monitoring; reporting STRs, CTRs, and transactions involving counterfeit notes; sharing other legally required information; and serving as liaison with enforcement agencies, banks, and other institutions involved in AML/CFT efforts. This description of the principal officer's responsibilities corresponds with the role as defined in the PML Rules, and does not include responsibility for overall AML/CFT compliance. The RBI Circular dated 11 September, 2009, amending the Master Circular for commercial banks, explicitly requires that the Principal Officer and other appropriate staff should have timely access to transaction monitoring and customer identification information. The September 2009 Circular further provides that the Principal Officer must be able to act independently and report directly to the senior management or to the Board of Directors. RBI circulars for NBFCs and RRBs (13 November 2009), UCBs (16 November 2009) add these requirements for these RBI-supervised institutions.

614. The RBI circular for authorised money changers (27 November 2009) specifies a broad compliance role for the Principal Officer. The position is charged with responsibility not only for monitoring and reporting transactions, but also for "developing appropriate compliance management arrangements across the full range of AML/CFT areas, e.g., CDD, record-keeping, etc"⁵⁹. In addition, the Principal Officer must be able to act independently and report directly to senior management or the Board of Directors. The circular directs that the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information; transaction records; and other relevant information.

Securities sector

615. The SEBI Master Circular in effect until 12 February 2010 requires registered intermediaries to issue AML/CFT policies and procedures that cover the current legal requirements for record retention, reporting (and other co-operation with law enforcement, including disclosure of information), customer acceptance and CDD, monitoring and detection of unusual and suspicious transactions. Further, securities intermediaries must adopt risk-based customer acceptance and CDD policies and procedures; communicate all AML/CFT policy and procedures to management and relevant staff; ensure that they are understood by

⁵⁹ Money Changing Activities Circular, par. 3 and Annex (F-Part-I), par. 4.12 (27 November 2009).

all employees who handle account information, securities transactions, money, and customer records; and train staff to guard against ML/FT. The Master Circular also requires intermediaries to regularly review their AML/CFT policies to ensure their effectiveness and to implement an internal audit or compliance function to ensure compliance with AML/CFT policies, procedures, and controls that includes sample testing. These requirements are further elaborated in the Master Circular issued in February 2010.

616. The SEBI guidance requires intermediaries to have an appropriate compliance structure in place. The September 2009 guidance also specifies that the Principal Officer “shall have access to and be able to report to senior management above his/her next reporting level or the Board of Directors” (par. 1(g)). SEBI guidance amending the Master Circular states that the “Principal officer/*money laundering control and other appropriate compliance, risk management and related staff members* shall have timely access to the customer identification data and other CDD information, transactions records and other relevant information” (par. 1(g) (1 September 2009)). This matter has been clarified in the most recent Master Circular (12 February 2010), which goes into considerable detail to emphasise intermediaries’ obligations to establish internal policies and procedures “that effectively serve to prevent and impede money laundering and terrorist financing”, considering the specific nature of its business, organisational structure, type of client and transactions, etc. The new Master Circular specifically requires the AML/CFT policies and procedures include an internal audit or compliance function to ensure compliance with the policies procedures and controls relating to the prevention of money laundering and terrorist financing.

Insurance sector

617. The IRDA Master Circular requires insurance companies to establish and implement a detailed AML policy that covers customer acceptance policies; customer identification procedures; transaction monitoring; a risk management framework; and record-keeping procedures. The AML policy must be approved by the insurance company’s board, reviewed and updated annually, and filed with IRDA. The IRDA Master Circular also requires insurance companies to integrate their agents into their AML program by adopting rules and regulations governing the AML/CFT performance of agents and making KYC norms and obligations a mandatory part of agent contracts. All insurance companies have filed the mandatory AML program/policy document with IRDA.

618. The IRDA Master Circular expressly requires insurance companies to designate a principal compliance officer, whose responsibilities include ensuring that the Board-approved AML programme is being effectively implemented (including by monitoring agents’ compliance) and that the insurance company’s employees and agents have appropriate resources and are well-trained to apply the AML programme. An IRDA Circular dated 24 August 2009 specifies that the compliance officer and other appropriate staff must have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

Adequately resourced and independent audit function

Institutions supervised by the RBI (including AMCs)

619. Under the RBI circulars, banks must also implement internal audit and compliance functions to evaluate and ensure adherence to their KYC policies and procedures, and the compliance function must provide an independent evaluation of the bank’s own policies and procedures, including legal and regulatory requirements. The RBI circulars do not explicitly require the independent audit function to include sample testing, but there appears to be nothing to prevent the audit function from having complete access to information within the institution in order to test compliance with the AML/CFT policy and procedures. The RBI Master Circular for SCBs and FIs, and the Circular for AMCs (27 November 2009) specifically mandate adequate resources for the independent audit function. Similar explicit requirements do not exist for other institutions supervised by the RBI, but are implied in the requirement to implement

an effective internal audit and compliance function to ensure adherence to AML/CFT policies and procedures.

Securities sector

620. The SEBI Master Circular requires intermediaries to implement an internal audit or compliance function to ensure compliance with AML/CFT policies, procedures, and controls that includes sample testing. The Master Circular is silent with regard to the independent character of the audit function and the fact that it must be adequately resourced. However, a previous SEBI Circular (22 August 2008) requires a half-yearly internal audit of stock brokers by independent qualified Chartered Accountants. Moreover, the Master Circular that came into effect on 12 February 2010 makes it clear that all AML/CFT measures—which would include the internal audit or compliance function—must be adequate and appropriate to effectively combat money laundering and terrorist financing, and instructs that senior management should be fully committed to establishing and implementing appropriate policies and procedures and ensuring their effectiveness and compliance with both all relevant legal and regulatory requirements and the spirit (and purpose) of the PMLA. Sufficient resources and independence would be essential components of this directive.

Insurance sector

621. The IRDA Master Circular was amended on 24 August 2009 to specifically point out that the principal compliance officer for AML guidelines should be at senior level and preferably not below the Head (Audit/Compliance) /Chief Risk Officer level and should be able to act independently and report to senior management (par. 3 (e) - 24 August 2009). The audit/compliance function is not expressly required to include sample testing, but there appear to be no obstacles to the audit function's obtaining access to information within the institution to test compliance.

Ongoing Compliance Training

Institutions supervised by the RBI (except AMCs)

622. RBI circulars require banks and other RBI-supervised institutions to establish an ongoing employee training programme to ensure that employees fully understand KYC policies and procedures and implement them consistently. The training programme must be specifically tailored to the different requirements for frontline staff, compliance staff, and staff dealing with new customers (see RBI Master Circular and RBI circulars for other banks and NBFCs).

Securities sector

623. The SEBI Master Circular requires intermediaries to have ongoing AML/CFT employee training programmes, addressing the different requirements of frontline staff, compliance staff, and staff dealing with new customers. The training must include not only the relevant AML/CFT procedures, but also the rationale behind the AML/CFT guidelines, obligations and requirements, and seek to ensure their consistent application.

Insurance sector

624. The IRDA Master Circular requires in-house AML training for all agents and sets forth in considerable detail essential training components that must be provided for specific categories of employees, including: new employees; sales/advisory staff (front-line staff); processing staff; and administration/operations supervisors and managers.

Authorised Money Changers

625. Authorised money changers are subject to the same training requirements as other RBI-supervised institutions (see RBI circular 27 November 2009).

India Post

626. India Post is subject to the same training requirements as other authorised money changers, with respect to money changing activities (see RBI circular 27 November 2009), but these represent only a minute portion of India Post's financial activities.

Screening procedures when hiring employees

Institutions supervised by the RBI (except AMCs)

627. RBI guidance instructs banks and other financial institutions to adopt adequate screening mechanisms as part of their personnel recruitment/hiring process in order to keep criminals from abusing the financial system for ML/TF purposes.

Securities sector

628. The SEBI Master Circular instructs registered intermediaries to have adequate screening procedures in place to ensure high standards when hiring employees. Further, it directs intermediaries to identify the key positions in their organisations with regard to ML/TF risks and the size of their business and ensure that the employees filling these key positions are suitable and competent to perform their duties. In addition, SEBI requires certification of "associated persons" for mutual fund distributors, derivatives traders, and depository participants". The certification process requires all persons engaged in handling investors' money, assets, and complaints; dealing with operational risk; attending to compliance; and persons responsible for management of intermediaries to demonstrate minimum professional standards in order to maintain their registration with SEBI (Certification of Associated Persons in Securities Markets Regulations, 2007).

Insurance sector

629. The IRDA Master Circular requires insurance companies to carefully monitor the selection process for agents, with an eye to the AML/CFT risks of the insurance business, including the agent's role in bringing in non-face-to-face business with policy holders, and to adopt adequate screening procedures when hiring employees.

Authorised Money Changers

630. The RBI circular for AMCs requires them to adopt adequate screening mechanisms as part of their personnel recruitment/hiring process, as a corollary of other AML/CFT requirements intended to combat abuse the financial system for ML/TF purposes.

India Post

631. See requirements for Authorised Money Changers, above. The RBI requirements apply only to India Post's minimal money changing activities.

Additional elements

632. The Principal Officer is generally in a position to report to top management or the Board of Directors with respect to the AML/CFT compliance issues. RBI circulars require banks and other RBI-supervised financial institutions to designate a senior management officer as the principal officer. The SEBI guidance has been further completed on 1 September 2009 with a provision that the principal officer

shall have access to and be able to report to senior management above his/her next reporting level or the Board of Directors, and this requirement is continued in the 2010 Master Circular. The provision in the IRDA guidance regarding the appointment of a Principal Officer includes the requirement that this person should be able to act independently and to report to senior management.

Recommendation 22

Banking sector

633. RBI circulars for SCBs and FIs, and NBFCs expressly provide that to the extent host country laws and regulations permit, the AML/CFT requirements set forth in the RBI guidelines shall apply to branches and majority owned subsidiaries located abroad, especially in countries that do not or insufficiently apply the FATF Recommendations. When local applicable laws and regulations prohibit implementation of the RBI AML/CFT guidelines, the covered institutions must notify the RBI of this situation. In addition, where the AML/CFT requirements of India and host countries differ, branches and overseas subsidiaries in host countries are required to apply the more stringent requirements, to the extent that local (*i.e.* host country) laws and regulations permit.

Securities sector

634. SEBI guidance similarly requires the branches and subsidiaries of securities market intermediaries located abroad to apply SEBI's AML/CFT measures, to the extent that local laws and regulations permit, especially, in countries which do not or insufficiently apply the FATF Recommendations. When local applicable laws and regulations prohibit implementation of the SEBI AML/CFT guidelines, the covered institutions must notify the regulator of this situation. If there is a variance in the KYC/AML standards prescribed by SEBI and those of the host country, branches and overseas subsidiaries are required to adopt the more stringent requirements of the two⁶⁰ (par. 5 of transmittal letter accompanying SEBI Master Circular (19 December 2008))⁶¹.

Insurance sector

635. India has not applied the requirements of Recommendation 22 to the insurance sector, since insurance companies are not permitted to conduct business overseas through branches or subsidiaries. Rather, insurance companies can only operate overseas through representative offices, which do not transact business, but simply function to promote awareness of Indian insurance products in non-resident populations. IRDA Circular (Office/06-07, dated 8 January 2007) governs the opening of representative offices abroad, and specifically prohibits underwriting outside India or other than in INR.

Authorised Money Changers

636. RBI guidance for money changers imposes the same requirements for overseas branches and subsidiaries as applied to SCBs and FIs, and NBFCs (par. 4.11 (27 November 2009)). AMCs do not have overseas branches or subsidiaries.

⁶⁰ Unlike RBI's requirements governing the banking sector's overseas branches/subsidiaries, the SEBI guidance does not expressly condition this requirement for overseas branches/intermediaries to apply the more stringent of SEBI or local AML/CFT standards on its being permitted by local laws and regulations.

⁶¹ Indian authorities informed the assessment team that the transmittal letter is considered an integral part of the Master Circular and its provisions are legally binding. The requirement is included in the 2010 Master Circular.

Additional elements

637. Indian financial institutions that are subject to the Core Principles are required to apply consistent CDD measures at the group level, taking into account the customer's activity with the various branches and majority owned subsidiaries worldwide.

Implementation and effectiveness

Recommendation 15

638. The PML Rules require all covered institutions to establish and maintain internal AML/CFT procedures, policies and controls that cover CDD and record retention, and to communicate these to their employees. While the PML Rules do not expressly require internal AML/CFT procedures, policies and controls to address the detection and reporting of unusual and suspicious transactions, they do require the appointment of a Principal Officer to handle the reporting function, which implies a need for procedures, policies and controls addressing the identification and reporting of unusual and suspicious transactions. In any event, OEM in the banking, securities, and insurance sectors requires covered institutions to establish and maintain effective risk-based AML policies and procedures regarding: customer acceptance policy; customer identification procedures; transaction monitoring; and risk management, and record retention.

639. For the banking sector, the RBI guidance addresses many of the criteria established by Recommendation 15 but does not require a money-laundering compliance officer, only a reporting officer.

640. The guidance in the securities sector satisfies Recommendation 15's criteria.

641. In the insurance sector, OEM requires insurance companies to establish an independent audit/compliance function, but does not provide that the audit function must include sample testing, although there appears to be no obstacles to the audit function's obtaining access to information to test compliance. The role of the principal compliance officer for insurance companies is described broadly to include responsibility across the full range of AML/CFT policies and procedures, and the compliance officer and other appropriate staff must have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

642. The application of the PMLA to India Post, including AML/CFT training and programmatic requirements, has not yet been effectively implemented.

Recommendation 22

643. India has fully implemented the requirements of Recommendation 22 with respect to foreign branches and subsidiaries of relevant banks, securities intermediaries and authorised money changers. The Recommendation is not applicable to India's insurance sector, since insurance companies are not legally permitted to conduct business overseas through branches or subsidiaries.

3.8.2 Recommendations and Comments

Recommendation 15

644. It is recommended that the Indian authorities:

- Extend the responsibilities of the Principal Officer in the banking sector beyond the STR and other reporting to overall compliance.
- Expressly provide that the audit function in all sectors should be independent and adequately resourced.

Recommendation 22

645. There are no recommendations with regard to Recommendation 22.

3.8.3 Compliance with Recommendations 15 & 22

| | Rating | Summary of factors relative to s.3.8 underlying overall rating |
|------|--------|--|
| R.15 | LC | <ul style="list-style-type: none"> The role of the principal officer in the banking sector (except for AMCs) is defined in terms simply of STR and other reporting, and does not extend to overall compliance. There is no express requirement that the audit function in the securities sector should be adequately resourced, and the resource issue is not expressly addressed in insurance sector. |
| R.22 | C | This Recommendation is fully observed. |

3.9 Shell banks (R.18)**Recommendation 18****3.9.1 Description and Analysis**

646. Although there are no specific provisions in the Banking Regulation Act or elsewhere prohibiting the establishment of shell banks, the requirements for establishing a bank set forth in the Banking Act and related regulations and the licensing process for banks established by the RBI ensure that shell banks do not operate in India.

647. Par. 2.12(b) of the RBI Master Circular stipulates that banks should refuse to enter into a correspondent relationship with a “shell bank” (*i.e.* a bank that is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). In addition, the provisions in the RBI Guidance indicate that banks should also “guard against” establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. Although mandatory in nature, the formulation of this last provision is somewhat vague. Based on the RBI’s powers set out in sections 46 and 47A of the Banking Regulation Act, the RBI can indeed take penal action if during a supervisory visit it is identified that a bank has no policies or controls in place to prevent the possibility of establishing a relationship with a shell bank or to satisfy itself that foreign respondents do not permit their accounts to be used by shell banks. The assessment team however, has concerns regarding the effectiveness of the regime because it has not been clarified what kind of measures or internal procedures financial institutions currently have in place to enable them to identify and avoid relationships with shell banks.

3.9.2 Recommendations and Comments

648. It is recommended that the RBI provides guidance to financial institutions regarding measures that should be in place in order for financial institutions to satisfy themselves that they are not entering into relationships with shell banks or that their foreign respondent institutions do not permit their accounts to be used by shell banks.

3.9.3 Compliance with Recommendation 18

| | Rating | Summary of factors relative to s.3.9 underlying overall rating |
|------|--------|---|
| R.18 | LC | <ul style="list-style-type: none"> There is no guidance for financial institutions regarding measures that should be in place to satisfy themselves that they are not entering into relationships with shell banks or that their foreign respondent institutions do not permit their accounts to be used by shell banks. |

Regulation, supervision, guidance, monitoring and sanctions

3.10 The supervisory and oversight system - competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)

3.10.1 Description and Analysis

Authorities/SROs roles and duties & Structure and resources – R. 23, 30

Designated supervisory authorities and application of AML/CFT measures – R.23

649. There are three primary financial regulators in India: the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority (IRDA). The FIU-IND also has inspection and enforcement powers with respect to the financial sector reporting on AML/CFT matters. Under the original July 2005 PML Rules, only the RBI and the SEBI were recognised as competent authorities for AML/CFT regulation and supervision, with the responsibility to specify the manner in which institutions should comply with the various obligations under the Rules. However, the IRDA was subsequently incorporated as the AML/CFT regulator and supervisor for the insurance sector through an amendment to the PML Rules in December 2005. The range of competent AML/CFT regulators/supervisors was further expanded by the amendment of the PML Rules in November 2009, which introduced the definition of a “regulator” as a person, authority or government which is vested with the power to license, authorise, register, regulate or supervise the activity of banking companies, financial institutions or intermediaries. This definition does away with the need to specify individual agencies by name. While each regulator has been designated as the competent authority under the PML Rules to introduce specific compliance obligations, the circulars that bring into force those obligations are issued under the provisions of the respective regulatory laws (e.g. the Banking Regulation Act in the case of the RBI, etc).

650. As indicated at the start of Section 3 of this report, there is an over-arching scope issue in that the Commodity Futures Brokers are not subject to AML/CFT requirements. This minor gap in the scope of the supervisory framework affects the ratings for the Recommendations 17, 23 and 29.

FIU-IND

651. Chapter VIII of the PMLA provides for the appointment of specified Authorities for the purposes of the PMLA, and section 49 states that the Central Government may appoint such persons as it think fit for the purposes of being Authorities under the PMLA.

652. As set out in section 2.5 above, on 18 November 2004, the Government of India issued an Office Memorandum (OM) to establish the FIU-IND, the purpose of which is to co-ordinate and strengthen the collection and sharing of financial intelligence. The OM states that the FIU-IND is established as an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister. The OM also establishes an officer of the rank of Joint Secretary to the Government of India to be the Director of the FIU-IND. Subsequently, on 1 July 2005, the Government of India published in the Gazette a Notification granting exclusive and concurrent powers, contained in the PMLA, to the Director of the FIU-IND, including the power:

- a. to receive information on transactions from the reporting entities within the prescribed time;
- b. to call for records and make such inquiry or cause such inquiry to be made, as he thinks fit;
- c. to levy a fine to the reporting entities for failure to comply with the record-keeping and reporting requirements; and

- d. of discovery and inspection, enforcing the attendance of any person, compelling the production of records, receiving evidence on affidavits, issuing commissions in relation to the power to impose fines.

The Reserve Bank of India (RBI)

653. The RBI is designated as the regulator of a wide range of institutions, with its powers and responsibilities laid down in both its own governing legislation and the various sector-specific statutes. Certain types of financial institutions as defined in the FATF Methodology are supervised by the RBI, with the exception of some functionalities of India Post. The India Post falls to the government to oversee its deposit-taking activities – this is explained in detail below. Money remitters and payment system operators are recent additions to the institutions covered under the PMLA. There are six separate departments within the RBI which have regulatory responsibilities for prudential and AML/CFT regulation. In addition, there is the Department of Banking Supervision which is responsible for supervision of commercial banks. These are listed in the following table.

| Class of entities | RBI Department |
|--|---|
| Scheduled Commercial Banks | Department of Banking Supervision (supervisor) and Department of Banking Operations and Development (regulator) ⁶² |
| Urban Co-operative Banks | Urban Banks Department |
| Regional Rural Banks/State Co-operative Banks/District Central Co-operative Banks | Rural Planning and Credit Department (regulator) and NABARD (supervisor) |
| Non-Banking Financial Companies | Department of Non-Banking Supervision |
| All-India Financial Institutions (e.g. NHB, NABARD, EXIM Bank and SIDBI) | Department of Banking Operations and Development |
| Authorised Persons Money Changers (includes money changers and Indian agents of Money Transfer Service Providers) | Foreign Exchange Department |
| Payment System Operators (e.g. VISA, MasterCard, etc.) | Department of Payment and Settlement Systems |

654. Within the group of “All India Financial Institutions”, there are two sub-regulators. The National Bank for Agriculture and Rural Development (NABARD) is responsible for supervising compliance by the rural co-operative sector with the relevant RBI guidance, and carrying out inspections of these institutions under the provisions of the Banking Regulation Act. This means that, while the Rural Planning and Credit Department has responsibility for issuing the circulars that lay down the obligations for this sector, it does not maintain its own supervisory staff to carry out compliance and monitoring. The National Housing Bank (NHB) is a wholly owned subsidiary of the RBI and was set up to function as a principal agency to promote housing finance institutions. The NHB regulates and supervises the housing finance system of the country and is empowered to determine the policy and give directions to the housing finance institutions and their auditors under the National Housing Bank Act (NHB Act). The NHB has issued a range of

⁶² The Department of Banking Operations and Development as the regulator creates the preventive rules and regulations for scheduled commercial banks while the Department of Banking Supervision supervises financial institutions, including on-site inspections, to ensure compliance with the rules and regulations. Similarly in the case of Regional Rural Banks/State Co-operative Banks/ Central Co-operative Banks at District level, there is a separate regulator and supervisor.

AML/CFT circulars to the housing finance institutions. Both the NABARD and the NHB are, in turn, overseen by the RBI.

The Securities and Exchange Board of India (SEBI)

655. The SEBI is responsible, under the SEBI Act, for the licensing and supervision of the stock exchanges, market intermediaries (such as stock brokers, underwriters, portfolio managers and investment advisers), depositories and custodians, and collective investment schemes. The SEBI's primary focus is to ensure investor protection, market stability and to counter market manipulation. Further, its powers extend to AML/CFT compliance in the securities market.

656. The SEBI has the authority to delegate some of its compliance functions to the stock exchanges, which are deemed to be self-regulatory organisations, based on section 19 of the SEBI Act. However, the SEBI retains responsibility for the regulatory oversight of the exchanges themselves. There are two stock exchanges that account for nearly all the transactions in the equity and derivative segments: the Bombay Stock Exchange (BSE) and the National Stock Exchange (NSE). SEBI has delegated powers to these two exchanges to ensure that their members adhere to the SEBI regulations and instructions. In addition to the directives issued by SEBI mandating the exchanges to carry out inspections of brokers every year, both exchanges are authorised by their own by-laws, regulations and rules to carry out inspections of their members. The legal validity of these by-laws and rules can be found in sections 4 and 9 of the Securities Contract Regulation Act, 1956. The BSE and the NSE report to SEBI regarding the compliance observed by their members, and a formal co-operation and co-ordination mechanism is in place in this regard. In addition, when there is a suspicion of serious breaches of the SEBI circulars, SEBI and the exchanges conduct joint inspections and investigations. These joint inspections are in addition to the inspections conducted by SEBI solely.

657. A very similar structure exists with respect to the function of the Depositories and their supervision over their members, known as depository participants. The SEBI regulates and oversees the functioning of the Depositories which are deemed to be self-regulatory organisations much in the manner of the Exchanges. Participation in the Indian securities market requires an investor to create accounts with both a stockbroker and a depository participant, both of whom are entrusted with independent account opening processes and are obliged to conduct ongoing CDD.

Insurance Regulatory and Development Authority

658. The IRDA was set up in 2000 to regulate, promote and ensure orderly growth of the insurance business and re-insurance business. The legislative framework for this sector is contained in the Insurance Act, 1938 and the IRDA Act, 1999. The IRDA regulates and supervises insurance companies, insurance intermediaries and other organisations connected with the insurance business.

659. Section 14 of the IRDA Act lays down various powers and functions of the Authority, which include calling for information, undertaking inspections, conducting enquiries and investigations, including audit, of insurers, insurance intermediaries and other organisation connected with the insurance business. Section 33 of the Insurance Act empowers the Authority to direct any person in writing to investigate the affairs of any insurer. The Insurance Act also empowers the Regulator to impose sanctions for non-compliance with regulatory requirements by insurers, intermediaries, insurance intermediaries, agents and corporate agents. These sanctions range from monetary penalties to suspension or cancellation of licences. Through the December 2005 amendment to the PMLA Rules, the IRDA was given the specific responsibility to issue AML/CFT guidelines, which are issued under section 34 of the Insurance Act.

Ministry of Finance

660. India Post is regulated by two regulators depending on the financial services it offers: the deposit taking and domestic money order activities are regulated by the Ministry of Finance while the international remittances activities, which India Post undertakes as an Authorised Person under the Foreign Exchange Management Act (FEMA), are licensed and regulated by the RBI. As indicated above, India Post also offers life insurance products in an agency capacity, but it is not directly supervised by the IRDA in this regard, since IRDA focuses its supervision on the insurance company that provides the products sold by India Post.

661. Regulation of India Post's deposit-taking and domestic money order activities falls within the purview of the Ministry of Finance, Department of Economic Affairs rather than the RBI. India Post indicated that, there is an ongoing discussion taking place currently regarding the Ministry of Finance's regulatory role in general, and in particular, the supervision of AML/CFT of India Post, which became subject to the PMLA in June 2009.

662. As indicated in the preamble to this section, the Department of Posts within the Ministry of Communications and IT issued an office memorandum in January 2010 outlining some basic AML/CFT requirements in respect of STRs, record-keeping and the role of the compliance officer. This was subsequently replaced by new office memoranda issued on 12 and 23 April by the Ministry of Finance's Department of Economic Affairs, but this guidance clearly falls outside the scope of this mutual evaluation. In addition, the Ministry of Finance has not yet undertaken any inspections of India Post and hence, it is clearly too early to assess the effectiveness of the regulatory and supervisory system in place for India Post. It should however be noted that India Post is subject to an independent audit by the Comptroller and Auditor General of India, as most other government departments, and has accountability to Parliament.

Structure and resources of supervisory authorities – R.30*The Reserve Bank of India (RBI)*

663. *Structure, funding and staff:* The RBI, which was constituted under the Reserve Bank of India Act, 1934, is the nation's central bank. Although it has operational independence from the Central Government and it enjoys freedom from influence or interference, the Government has extensive powers to appoint and remove members of the Board (sections 8 and 11 of the RBI Act). Also, under section 7(1) of RBI Act, the Central Government may, after consultation with the Governor, give direction to the Bank when it considers it necessary and in the interest of the public. The regulation and supervision of banking companies are entrusted to the RBI under Banking Regulation Act, 1949. Under section 52 of the Banking Regulation Act, the Banking Division (now the Department of Financial Services) within the Ministry of Finance has the general authority to make rules (after consulting with the RBI) to give effect to the provisions of the Act.

664. The RBI as a whole seems adequately funded and structured, and has sufficiently technical and other resources to perform its duties. The number of supervisory staff and respective budget allocation for 2009/2010 in the various departments of the RBI is shown in the following table.

| Supervisory Resources involved in AML/CFT | No. of staff | Budget for 2009-2010 | |
|---|--------------|----------------------|--------|
| | | INR mn | USD mn |
| Department of Banking Supervision | 650 | 328.7 | 6.57 |
| Department of Non-Banking Supervision | 337 | 117.0 | 2.34 |
| Urban Banks Department | 400 | 258.1 | 5.17 |
| Foreign Exchange Department | 80 | 197.3 | 3.95 |
| Department of Payment and Settlement Systems | 38 | 293.8 | 5.88 |
| | | | |
| National Housing Bank | 12 | | |
| National Bank for Agriculture and Rural Development | 349 | | |

665. These officers are all permanent staff of the RBI and are recruited through an all-India competitive examination. All staff in the supervisory departments (RBI, NABARD, and NHB) is involved in supervising and monitoring AML/CFT compliance, as it forms an integral part of the RBI's routine prudential supervision programme. The budget of all the departments of the RBI is decided internally by the Bank, without any government involvement. The budget is funded directly from the income of the RBI, and there is no supervision levy imposed on the financial institutions. Major sources of income for the RBI are from (i) the deployment of foreign currency assets and gold and (ii) interest on domestic securities and market operations.

666. *Professional standards:* Staff of the RBI is governed by the Reserve Bank of India (Staff) Regulations, 1948, issued by the Central Board of the RBI. These Regulations, which include integrity standards in Chapter IV, are binding in nature and an employee who breaches the provisions under the Regulations, displays negligence or inefficiency, commits a breach of discipline, or is guilty of any other act of misconduct is liable to penalties ranging from a reprimand to dismissal from the service depending on the severity of the breach. The annual performance assessment also focuses on the integrity of the employee. In addition, the employees are required to follow the anti-corruption guidelines issued by the Central Vigilance Commission (CVC).

667. *Training:* RBI staff is provided with regular and relevant training on AML/CFT in the different departments. Between 2006 and 2009, 110 AML/CFT familiarisation programmes were organised for the officers, both in-house and in the RBI's two training colleges. The training needs are identified by the RBI's training institutes: the Reserve Bank Staff College (RBSC) in Chennai and the College of Agricultural Banking (CAB) in Pune. The RBSC was established to provide training to the RBI's own officers in junior and middle management cadres, and specialised development of officers in the senior management cadre. The CAB was originally set up with a focus on training of the senior and middle level officers of the rural and co-operative credit sectors, but has in recent years diversified and expanded the training to cover areas relating to non-banking financial companies, human resource management and information technology. In addition, the RBI has four Zonal Training Centres (ZTCs), which focus on the improvement of skills across all cadres of the RBI.

668. Supervisory officials also follow specialised training in various international institutions, including the US Federal Reserve. A total number of 29 overseas training programmes have been attended by RBI officials. The officers of RBI are seconded to commercial banks on selective and reciprocal basis in order to expose them to the functioning of commercial banks. An MOU between the Central Government, the State Government and the NABARD ensures that NABARD is provided with training and capacity

building. NHB officials have attended training programme/workshops conducted by FIU-India and RBI. In the past, NHB officials have also been nominated to the programme conducted for the officials of HFCs on KYC.

The Securities and Exchange Board of India (SEBI)

669. *Structure, funding and staff:* SEBI is a statutory body established by the SEBI Act and the structure and constitution of the SEBI Board is laid down in section 4(1) of this Act. It should be noted that the operational independence from the Central Government is also a characteristic of the SEBI. Chapter IV of the Act contains provisions relating to powers and functions of SEBI, while Chapter VI specifies the funding arrangements for SEBI, which includes income sourced from grants, fees and charges made under the SEBI Act, and any other sources prescribed by government. SEBI has a staff of 490, of which 90 are devoted to investigations and surveillance, and 62 to inspections of exchanges and intermediaries, including for AML/CFT purposes.

670. SEBI's funding is entirely from the charges made on the securities market and is not dependent on government allocations. Allocation of funding within SEBI on various functions such as supervision, investigation and inspection is purely a matter for SEBI and there is no government involvement. The budget estimates for the year 2009/10 as approved by the SEBI Board is as depicted in the table below:

| | Particulars | INR mn | USD mn |
|---|---------------------------|--------|--------|
| 1 | Total Income | 2 329 | 46.6 |
| 2 | Total Revenue Expenditure | 1 000 | 20.0 |
| 3 | Total Capital Expenditure | 1 289 | 25.8 |

671. Similarly, the stock exchanges have dedicated staff to conduct inspections of members, including compliance for AML/CFT purposes. For example, in case of the NSE, the structure of the inspection team and the resources for conducting inspections involves two vice-presidents, two assistant vice-presidents, one manager and eight assistant managers. The cost of supervisory departments is funded through the Internal Accruals of the Exchanges, like transaction charges. The BSE amount budgeted for supervision for the financial year 2009-2010 was INR 5.83 million (USD 116 600), excluding staff costs of INR 37.93 million (USD 758 600), and the NSE spent an amount of INR 17 million (USD 340 000), excluding staff costs of INR 45.95 (USD 919 000), until December 2009 for supervisory purposes. The depositories' funding requirements for inspection and surveillance activities are met from the overall budget of the depositories. This is funded out of the existing capital and earnings of the depositories (comprising levies on the participants, etc). The Central Depository Services (India) Limited's (CDSL) annual inspection budget for the year 2009-10 is approximately INR 7 million (USD 0.14 million).

672. *Professional standards:* The SEBI (Employees Service) Regulations, 2001 require each employee to maintain absolute integrity, good conduct and discipline; and maintain devotion and diligence to duty. All SEBI employees are also required to sign a declaration of fidelity and secrecy in which they declare to faithfully, truly and to the best of their skills and abilities execute and perform the duties required of them as an employee of the SEBI. Under Regulation 79, an employee who commits a breach of any regulation of the Board; displays negligence, inefficiency or indolence; knowingly does anything detrimental to the interests of the Board or in conflict with its instructions; commits a breach of discipline; or is guilty of any other act of misconduct, shall be liable to a range of penalties.

673. *Training:* Staff of the SEBI have attended various training sessions, workshops, conferences and seminars on AML and CFT, including: (a) a broker-dealer AML programme organised by the US Security and Exchange Commission; (b) a joint India-IMF workshop on AML and CFT; (c) a South Asia regional

conference on CFT in the charitable sector; (d) a bilateral US-India FATF AML/CFT Workshop; and (e) study visits of the Hong Kong, China Stock Exchange and Securities Commission; and the Singapore Stock Exchange and the Monetary Authority of Singapore to study surveillance and AML/CFT measures. On-the-job training is provided to staff in the inspection team for stock exchanges. The induction programme for officers of stock exchanges (in which inspection staff also participate) covers AML/CFT compliance. For example, in the case of the NSE, during the period April-November 2009, 14 training programmes were organised by the exchange for its trading members. Additionally, one refresher programme covering AML compliance was conducted exclusively for the Inspection staff during the same period.

Insurance Regulatory and Development Authority

674. *Structure, funding and staff:* The IRDA was established under the IRDA Act. It has operational independence from the Central Government, in a similar vein as the RBI and the SEBI under section 18 and 10 of its governing act. IRDA has a total strength of 126, including the Chairman, full-time members of the Authority and staff seconded to the Authority. The Authority is organised into various departments to discharge its functions of policyholder's protection, regulation and orderly growth of the insurance industry. While a team of only four officials, including one full-time member of the Authority, is involved in monitoring compliance with the AML/CFT guidelines *per se*, the IRDA states that other specialised departments (e.g. life, non-life, actuarial and inspection) also play their part in compliance checks on the AML/CFT regime in the industry. For example, IRDA's general inspection department, comprising of 9 staff members, carries out focused/market conduct inspections, including compliance checks on AML/CFT guidelines. The life insurance department, comprising of 10 staff members, work on the follow-up action on the findings pertinent to AML/CFT issues which are identified as part of the market conduct inspections. The actuarial department, comprising of 12 staff members, clears all the life insurance products which are mandatorily filed with the Authority (e.g. proposal forms containing a checklist of documents required for proof of identity, residence, and income). IRDA's staff strength has been growing in pace with the regulatory/supervisory requirements of the regulated industry. Technology has been used to supplement the Regulatory/Supervisory Effectiveness. The Authority strongly recognises the need to replenish its human resources through the induction of qualified experts for effective supervision as well as expand and grow with the developments and growth in the industry. Further many initiatives are in the offering to automate the operational and analytical requirements of the various functions.

675. The manner of the IRDA's funding is prescribed in Chapter V of the IRDA Act. Section 16(1) speaks of the constitution of an "Insurance Regulatory and Development Authority Fund" which is made up of all government grants, fees and charges received by the Authority; sums received by the Authority from such other sources as may be decided upon by the Central Government; and the percentage of prescribed premium income received from the Insurer. Section 16(2) stipulates that the Fund shall be applied for the salaries and remuneration of the officials and employees of the Authority; and meeting other expenses of the Authority in connection with discharge of its functions and for the purposes of the IRDA Act. The IRDA's budget for the year 2009-10 is INR 1282mn (USD 25.6mn), comprising receipts from insurers, intermediaries and interest from the investments by IRDA.

676. *Professional standards:* Staff of the IRDA is subject to the IRDA (Conditions of Service of officers and other employees) Regulations, 2000, which (Regulation 29) requires IRDA officials to maintain strict confidentiality, honesty and code of conduct.

677. *Training:* The IRDA set up its Institute of Insurance Risk and Management (IIRM) in 2002 jointly with the State Government of Andhra Pradesh, where various training programmes for staff are conducted, including induction training to new employees of IRDA. Training on AML/CFT is part of such course programmes. Apart from training in IIRM, IRDA staff undergoes training programmes on various issues both within and outside India. 15 officers were sent to NAIC, USA for an internship of 6-8 weeks

covering on-site and off-site monitoring of insurance companies. As a policy, the IRDA is now sending officers to the NAIC on an internship programme (which is conducted twice a year).

678. With specific reference to AML/CFT, IRDA staff has been sent to training sessions organized by IMF, US embassy, FIU-IND etc. In-house training is organized on need basis. For example, inspection teams are being trained in-house on AML/CFT inspection procedures, and an inspection manual has been developed by the AML section

Authorities Powers and Sanctions – R. 29, 17

Supervisory powers – R.29

The Reserve Bank of India (RBI)

679. *Power to monitor and ensure compliance:* The RBI has been empowered by different Acts to regulate a broad cross-section of financial institutions, with the exception of India Post which falls under the purview of the government. Under the PML Rules, and various sections of the Banking Regulation Act, RBI Act and the FEMA, the RBI issues directions on compliance with the PMLA to commercial banks and all the other financial institutions that it regulates. The table below illustrates the different laws that empower the RBI to issue directions:

| PMLA Definition | Class of entities | Regulatory Department/Institution | Legislative power to issue directions |
|---|--|--|---|
| Section 2(e) of PMLA - "banking company" means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 applies and includes any bank or banking institution referred to in section 51 of that Act" | Scheduled Commercial Banks | Department of Banking Operations and Development | Section 35A of Part I of the Banking Regulation Act, 1949 |
| | Urban Co-operative Banks | Urban Banks Department | Section 35A of Part V of the Banking Regulation Act, 1949 (As Applicable to Co-operative Societies) |
| | Regional Rural Banks State Co-operative Banks/Central Co-operative Banks at District level (Regional Rural Banks incorporated under the Regional Rural Banks Act, 1976) | Rural Planning and Credit Department | Section 35A of Part V of the Banking Regulation Act, 1949 (As Applicable to Co-operative Societies) |
| Section 2(l) of PMLA, 2002 - "financial institution" means a financial institution as defined in clause (c) of section 45-I of the Reserve Bank of India Act, 1934 and includes a chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company" | Non-Bank Financial institutions | Department of Non-Banking Supervision | Section 45K and 45L of the Reserve Bank of India Act, 1934 |
| | All-India Financial institutions such as NHB, NABARD, EXIM Bank and SIDBI | Department of Banking Operations and Development | Section 35A of Part I of the Banking Regulation Act, 1949 |
| | Housing Finance institutions | National Housing Bank | Section 30A and 31 of the National Housing Act, 1987 |
| Section 2(da) PMLA (Amendment) 2009 - "Authorised Person" means an Authorised Person as defined in clause (c) of FEMA, 1999" | Authorised Money Changers such as FFMCs and Indian agents of Money Transfer Service Providers | Foreign Exchange Department | Sections 10(4) and 11(1) of the Foreign Exchange Management Act, 1999 |

| PMLA Definition | Class of entities | Regulatory Department/Institution | Legislative power to issue directions |
|--|--|--|---|
| Section 2(rc) of PMLA (Amendment) 2009 - "Payment system operator" means a person who operates a payment system and such person included his overseas principal. | Payment system providers such as VISA, Master Card, etc. | Department of Payment and Settlement Systems | Section 18 of the Payments and Settlement Systems Act, 2007 |

680. *Power to conduct inspections:* The RBI has broad statutory powers of inspection over the institutions that it supervises. For example, section 35 of the Banking Regulation Act allows the RBI at any time to carry out an inspection on the company, books and accounts. The inspection can extend to a director or an employee. It further allows the RBI to call for an external audit at any time. In addition, the Central Government can direct the RBI to carry out a special inspection, if it appears that the affairs of a banking company are being conducted to the detriment of the interests of its depositors.

681. Under section 35(6) of the Banking Regulation Act, the NABARD has powers to inspect banks under its supervision. In February 2009, the RBI instructed and highlighted the need for the NABARD to focus its supervisory efforts on the assessment of AML/CFT compliance with the RBI circulars on AML/CFT for RRBs, StCBs and DCCBs.

682. The NHB has powers to inspect HFCs under section 24 of the National Housing Bank Act. The NHB may at any time, or if directed by the RBI, inspect any institution to which the NHB has made any loan or advance or granted any other financial assistance, and its books, accounts and other documents.

683. The Department of Payment and Settlement Systems has the power to carry out audit and inspection under section 16 of the Payment and Settlement Systems Act (PSSA) which states that, for the purpose of carrying out its functions, the department can conduct (or appoint someone to conduct) audits and inspections of a payment system or its participants, and it shall be the duty of the system provider and the system participants to assist the RBI to carry out such audit or inspection.

684. Under section 12 of the FEMA, the RBI has the authority to inspect Authorised Persons to ensure, among other things, compliance with the directives issued under the Act.

685. *Power to compel production or to obtain access to records:* The RBI and the NABARD have broad powers, based on sections 27(2), 35(1)-(4) and 36(iii) of the Banking Regulation Act, to require regulated institutions to furnish information and documents on demand. There is no restriction on the type of information that may be requested and there is no need for a court order. Section 35 of the Banking Regulation Act provides for any director or employee to produce all such books, accounts and other documents in his custody or power and to furnish any statements and information relating to the affairs of the banking company as the inspector may require within such time as specified.

686. Section 24 of the NHB Act provides for every officer, employee or other person or persons in charge of the whole or part of the affairs of the institution to produce all such books, accounts and other documents in his custody or power, and to furnish within a specified time any information relating to the affairs of the institution as is required.

687. A similar power exists in section 45 of the RBI Act with respect to Non-Banking Financial Companies. The power to compel production of documents by NFBCs is vested in the provisions of Chapter III(B), section 45N (2) of the RBI Act, which states that it is the duty of every director, or member

of any committee or other body for the time being vested with the management of the affairs of the institution, or other officer or employee thereof, to produce for the inspecting authority all such books, accounts and other documents in his custody or power, and to furnish that authority with any statements and information relating to the business of the institution as that authority may require of him, within such time as may be specified by that authority.

688. Section 12(2) of the FEMA imposes an obligation on Authorised Persons to produce all such books, accounts and other records as may be required by the RBI, and to furnish such information as may be required.

The Securities and Exchange Board of India (SEBI)

689. *Power to monitor and ensure compliance:* Under section 11(1) of the SEBI Act, SEBI has the power to regulate the business of the stock exchange and securities market. Under this provision (as well as the PMLA Rules), SEBI has the power to issue circulars for stock exchanges and intermediaries, and under Chapter VI(A) of the SEBI Act (as well as the SEBI (Intermediaries) Regulations), there are provisions relating to penalties and adjudication in case of non-compliance by the supervised intermediaries and exchanges.

690. *Power to conduct inspections:* Section 11 of the SEBI Act empowers SEBI to call for information, undertake inspections, and conduct inquiries and audits of stock exchanges, mutual funds, persons associated with the securities market, intermediaries and self regulatory organisations in the securities market. Section 11C of the SEBI Act also provides for extensive powers to carry out special investigations where there is reason to believe that business is being conducted contrary to the interests of investors, or that a breach of the Act has occurred. Regulation 17 of the SEBI (Intermediaries) Regulations provides for inspections and disciplinary proceedings, including inspection of compliance with securities law and the relevant directions and circulars.

691. Similarly, the individual stock exchanges and depositories carry out annual inspections of their members. Overall, these inspections are aimed at ensuring compliance with the relevant instructions issued by SEBI and the exchanges, including the circulars issued on AML/CFT (circular NSA/INSP/5387 – 27/08/2004), and to ensure the completeness and integrity of the books and records. In addition to directives issued by SEBI mandating the exchanges to carry out inspections of brokers every year, the exchanges (both BSE and NSE) are authorised by their by-laws, regulations and rules to carry out inspections of their members. Depositories also conduct inspections of their participants on similar lines.

692. *Power to compel production or to obtain access to records:* SEBI has the authority to compel production of, or to obtain access to, records for supervisory purposes under section 11(2)(i) of the SEBI Act and Regulation 17(1) of the SEBI (Intermediaries) Regulations. This authority is not predicated on the need to require a court order. In addition, section 11(3) foresees that:

“The Board of SEBI shall have the same powers as are vested in a civil Court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters: (i) the discovery and production of books of account and other documents, at such place and such time as may be specified by the Board; (ii) summoning and enforcing the attendance of persons and examining them on oath; (iii) inspection of any books, registers and other documents of any person referred to in section 12, at any place; (iv) inspection of any book, or register, or other document or record of the company referred to in sub-section (2A); (v) issuing commissions for the examination of witnesses or documents.”

693. Further, under section 11(c)(3) of the SEBI Act, an appointed investigator may require any intermediary or any person associated with securities market in any manner to furnish such information to,

or produce such books, or registers, or other documents, or record before it or any person authorised by it in this behalf, as it may consider necessary, if the furnishing of such information or the production of such books, or registers, or other documents, or record is relevant or necessary for the purposes of its investigation.

Insurance Regulatory and Development Authority

694. *Power to monitor and ensure compliance:* Under section 14 of the IRDA Act, the IRDA has the duty to regulate, promote and ensure orderly growth of the insurance business. The AML guidelines were issued under the PML Rules and section 34 of the Insurance Act, 1938, which empowers the Authority to issue directions to the insurer in the public interest, to prevent detrimental activities against the interests of the policyholders and to secure the proper management of any insurer. Section 114A of the Act empowers the Authority to frame Regulations. Non-compliance with the AML guidelines may attract penalties under various provisions of the Insurance Act.

695. *Power to conduct inspections:* The IRDA is empowered under section 14(2)(h) of the IRDA Act to carry out inspections. The Act provides for the calling of information from, and the undertaking of inspection and investigations of insurers, intermediaries, insurance intermediaries and other organisations connected with the insurance business. Section 33 of the Insurance Act also empowers the IRDA to appoint inspectors to investigate the affairs of a licensee.

696. *Power to compel production or to obtain access to records:* The IRDA is empowered under section 14(2)(h) of the IRDA Act to call for information from insurers, intermediaries, insurance intermediaries and other organisations connected with the insurance business. Section 33 of the Insurance Act specifically imposes an obligation on insurers to produce all such books of accounts, registers and other documentation as the investigating authority may request. Section 34H of the Act provides powers of search and seizure, while section 110C gives powers to call for information from insurers relating to their business activities.

Powers of enforcement and sanctions – R.29 and 17

PMLA provisions applying to all covered institutions

697. Section 12 of the PMLA imposes obligations on all covered institutions to maintain records of, and furnish information on transactions. Section 13 empowers the Director of the FIU-IND to impose a fine of between INR 10 000 (USD 200) and INR 100 000 (USD 2 000) for each failure by covered institutions to comply with the provisions of section 12. Sections 70(1) and (2) of the PMLA, extend the application of administrative sanctions to both natural and legal persons. In case the contravention of the provisions of the PMLA was committed by a company, and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of any company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

698. During the financial year 2008-2009, a separate compliance section was created within the FIU-IND to act as the principal point to ensure compliance and initiate sanctions under the PMLA. The following steps were taken by the FIU-IND to improve compliance with the PMLA provisions:

- a. compilation of information related to AML policies, submission of CTRs and STRs, quality of data in the CTRs and the STRs, number of branches, status of computerisation of the covered institutions, and use of AML software;
- b. comparison between information received from external sources and submitted CTRs and STRs to identify non-compliance with the reporting obligation of the covered institutions;

- c. issue of advisory to reporting entities in cases where the reporting entity did not appear to have taken adequate measures to comply with its obligations;
- d. selection of reporting entities for prima facie review on the basis of comparison of the compliance history and other related information;
- e. monitoring of the improvement in compliance by the reporting entities under review; and
- f. levy of fines for non-compliance based on section 13 of the PMLA.

699. In this framework, information was identified regarding the failure to report by a bank of substantial CTRs. After giving reasonable opportunity to the bank to remedy the deficiencies and a further assessment of the circumstances, the FIU-IND imposed a penalty on the bank for its failure to comply with the reporting obligation in the PMLA.

Institutions supervised by the RBI (except AMCs)

700. Section 46(4) of the Banking Regulation Act states that if any provision of the Act is contravened or if any default is made in complying with any requirement of the Act or of any order, rule, or direction made or condition imposed there under, by any person, such person shall be punishable with a fine which may extend to INR 50 000 (USD 1 000) or twice the amount involved in such contravention or default where such amount is quantifiable. Where a contravention or default is a continuing one, the fine may extend to INR 2500 (USD 50) for every day during which a contravention or default continues. Section 46 may also lead to the criminal prosecution of the institution or its representatives, and it enumerates the circumstances in which the criminal sanctions route can be followed. Section 46(5) provides that where a contravention has been committed by a company, whoever at the time of the contravention was responsible for the conduct of the business of the company, shall be deemed guilty of the contravention and shall be liable to be proceeded against and punished accordingly. As far as failure to implement RBI directions is concerned, any person who wilfully makes a statement which is false in any material, knowing it to be false, or wilfully omits to make a material statement in compliance of any circular or direction issued by RBI, would be liable for imprisonment under section 46, for a term which may extend to 3 years. Since the RBI circulars are issued under section 35A of the Banking Regulation Act and the PML Rules (for banks and other financial institutions), these enforcement provisions may be applied for breaches of the AML/CFT obligations introduced under those circulars. These penalties apply equally to the institutions under the supervision of the RBI and the NABARD and can be imposed by courts at the instance of both supervisors.

701. Section 47A (1)(b) of the Banking Regulation Act also empowers the RBI to impose a penalty not exceeding INR 500 000 (USD 10 000) or twice the amount involved, and where the contravention continues, the penalty may extend to INR 25 000 (USD 500) per day. It would appear that the provisions of sections 46 and 47A are parallel. However, a close reading would indicate that the penal provisions of section 46(4) are applicable where a criminal complaint has been filed by the Bank, whereas the powers available under section 47A are more in nature of administrative power, under which the RBI can impose a penalty without approaching any Court. Usually, it is under this latter section that the RBI imposes penalties on various banks for non-compliance with the directions issued under section 35A of the Banking Regulation Act.

702. These sanctions do not only apply in relation to the legal persons that are financial institutions or businesses, but also to their directors and senior management. Section 46(5) states that where a contravention or default has been committed by a company, every person who, at the time the contravention or default was committed, was in charge of, and was responsible to, the company for the conduct of its business, as well as the company, shall be deemed to be guilty of the contravention or default, and shall be liable to be proceeded against and punished accordingly. Finally, the RBI informed

the assessment team that even though non-compliance with the AML/CFT requirements by itself is not stated as a ground for cancellation of a licence under section 22 of the Banking Regulation Act, continued violation of the directions issued by the RBI in this regard could be seen as conducting the affairs of the bank in a manner that is detrimental to the interest of the depositors, and would thus constitute a ground for cancellation of the licence by the RBI.

703. Section 49(4) of the NHB Act, 1987 states that, if any provision of the Act is contravened, or if there is any failure to comply with the Act, or any order, regulation or direction made or given or condition imposed under the Act, a person who is guilty of a contravention or default shall be punishable with a fine which may extend to INR 2 000 (USD 40). A recurring default attracts a further fine of INR 100 (USD 2) per day. In addition, under section 52A, if a default is committed by a housing finance institution, the NHB may impose a penalty not exceeding INR 5 000 (USD 100) or if the default relates to contravention of provisions on deposit-taking or commencement of business, or directions, a penalty not exceeding INR 500 000 (USD 10 000) or twice the amount of the contravention, whichever is more. If such a contravention or default continues, a further penalty may be imposed and this penalty may extend to INR 25 000 (USD 500) for each day of the contravention or default. No sanctions have been administered to date.

704. The NBFCs are regulated under the provisions of Chapter III(B) of the RBI Act. This gives the RBI the power to issue directions and impose sanctions which include, apart from monetary sanctions, the cancellation of the certificate of registration. Section 45IA states that the Bank may cancel a certificate of registration if the company, amongst other conditions, has failed to comply with any direction issued by the Bank or to maintain accounts in accordance with the requirements of any law or any direction or order issued by the Bank, or has failed to submit or offer for inspection its books of account and other relevant documents when so demanded by an inspecting authority of the Bank. If NBFCs fail to comply with these directions, the Bank can take action under section 58B (5)(aa) or section 58G (1)(b) which sets out a list of offences (including failure to comply with directions or to supply information) and accompanying penalties that are fines or terms of imprisonment for defaults and contraventions. The fines range from INR 2 000 (USD 40) per offence to INR 500 000 (USD 10 000) and different terms of imprisonment, up to three years, and can be applied for non-compliance of AML requirements. However, in terms of section 58G (5) and (6), if a complaint has been filed in court, no monetary fine can be imposed and vice versa.

705. Chapter VII of the PSSA provides for penalties and offences with respect to payment system operators. The sanctions range from monetary penalties up to INR 100 000/USD 2 000 or imprisonment up to three years. This extends to any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Authorised Money Changers

706. The AMCs are authorised under the FEMA, and the RBI circulars are issued under the provisions of this Act. Section 10(3) of the FEMA provides that a licence may be revoked by the RBI at any time if the RBI is satisfied that (a) it is in public interest to do so; or (b) the Authorised Person has failed to comply with the condition subject to which the authorisation was granted or has contravened any of the provisions of the Act or any rule, regulation, notification, direction or order made there under. Section 11(3) also provides for monetary penalties in cases where an institution fails to comply with directions issued by the RBI under sections 10(4) and 11(1) of the FEMA. In such circumstances, a fine can be levied which may extend to INR 10 000 (USD 200), and in the case of continuing contravention, an additional penalty may be applied of up to INR 2 000 (USD 50) for every day during which such contravention continues.

707. Responsibility for compliance within the AMC sector is divided between the RBI and the Directorate of Enforcement (ED), as set out in the following table.

| Role of the ED | Role of the RBI |
|---|--|
| <ul style="list-style-type: none"> • Investigation of contraventions of FEMA, including investigation of contraventions of licensing conditions • Investigations triggered by: (1) reference by RBI of cases suspected to involve FEMA contravention; (2) intelligence/specific information regarding contravention of FEMA; and (3) reports received from Authorised Persons through RBI regarding non-realisation of export proceeds • Issuance of show cause notice and adjudication of the offence, resulting in: (1) imposition of monetary penalties (of up to three times the value involved in the contravention), including on the Authorised Person [banks, authorised money changers etc.], if facts indicate deliberate participation in the unlawful activity by these persons; and (2) confiscation of the foreign exchange or Indian currency involved in the contravention | <ul style="list-style-type: none"> • Handling all procedural matters • Licensing of persons under various provisions of FEMA • Monitoring of export and import of foreign exchange out of or into India • Exercise of power of compounding of certain categories of contravention of FEMA upon payment of fine by the applicants |

Application of sanctions by the RBI

708. The sanctions available to the RBI, although relatively broad, appear to range from one extreme to the other. At one level, the monetary penalties provided under the various statutes appear to be very low, with some fines being the equivalent of less than USD 50 (even if this is cumulative on a daily basis for ongoing non-compliance). This cannot be considered to offer any disincentive to financial institutions. However, at the other extreme, criminal sanctions appear to be available in some cases for failure to comply with any of the directions issued by the RBI, but, in practice, no such criminal penalties have been imposed for AML/CFT deficiencies⁶³. The following table indicates the range of sanctions that have actually been applied by the RBI for breaches of the AML/CFT guidelines. These sanctions reflect a combination of cases where institutions have failed to comply with the guidelines in individual transactions, and instances where the RBI has identified serious cases of general failing in systems and controls. The RBI reports that the most common deficiencies identified during its examination programme, which lead to sanctions, are failure to abide by the RBI instructions for account opening and monitoring of transactions; violation of RBI instructions on observance of KYC guidelines while opening accounts of customers for Initial Public Offering (IPO) funding as well as the monitoring of sources of funds so used. Penalties have also been imposed for inadequate control mechanisms which have led to lapses in compliance with AML/CFT at branch level and are recurrent in nature.

⁶³ However, the RBI provided two recent instances, involving other matters, where criminal proceedings have been initiated under Section 46 of the Banking Regulation Act:

In the matter of Global Trust Bank (GTB) (before Metropolitan Magistrate, Mumbai): the RBI filed the captioned complaint against GTB and its directors for making false statements in the balance sheets and returns submitted to the Bank, and for criminal conspiracy punishable under the provisions of section 46(1) read with section 46(5) of the Banking Regulation Act and Section 120B of the Indian Penal Code.

In the matter of Nedungadi Bank (before Judicial First Class Magistrate, Kozhikode): The RBI filed a criminal complaint against Nedungadi Bank Ltd., and its former Chairman for contravention of the provisions of section 46(1) and (4) of Banking Regulation Act, and also the directions of the RBI relating to lending and investment in equities. The allegation is that Nedungadi Bank's Chairman allowed arbitrage trading beyond the permitted limit without exercising due diligence, and that the amount used by the bank in excess of the limit is not properly reflected in the returns and balance sheet of the bank.

Statistics: Sanctions applied by the RBI for breaches of the AML/CFT guidelines

| Year (to 31 March) | Category of agency ⁶⁴ | Penalties | | | Advisory notices | Show- cause notices | Warning letters | | | |
|--------------------------|----------------------------------|---------------------------------|-------------|--------------|---------------------|---------------------------|--------------------|--------------------------------|--------------------------------|--------------------------------|
| | | No. of agencies involved. | Amount | | | | | No. of agencies involved | No. of agencies involved | No. of agencies involved |
| | | | INR (mn) | USD (ooo) | | | | | | |
| 2004-2005 | Scheduled commercial banks | 2 | 1.0 | 20 | | 3 | 1 | | | |
| | Urban co-operative banks | | | | 52 | | | | | |
| | Authorised money changers | | | | | | 1 | | | |
| 2005-2006 | Scheduled commercial banks | 12 | 12.5 | 250 | 10 | 13 | | | | |
| | Urban co-operative banks | | | | 93 | | | | | |
| | Authorised money changers | | | | 1 | 1 | 1 | | | |
| 2006-2007 | Scheduled commercial banks | 2 | 2.0 | 40 | 1 | 4 | | | | |
| | Urban co-operative banks | 2 | 1.0 | 20 | 77 | 6 | | | | |
| | Authorised money changers | | | | | 3 | 1 | | | |
| 2007-2008 | Scheduled commercial banks | 2 | 2.0 | 40 | 1 | | | | | |
| | Urban co-operative banks | 11 | 3.8 | 76 | 33 | 7 | | | | |
| | Authorised money changers | 1 | .005 | 0.1 | | 4 | 2 | | | |
| 2008-2009 | Scheduled commercial banks | | | | 1 | | | | | |
| | Urban co-operative banks | 8 | 3.5 | 70 | 86 | 11 | 1 | | | |
| | Authorised money changers | | | | - | 5 | | | | |
| 2009-10 (9 months) | Urban co-operative banks | 3 | 0.3 | 6 | 20 | - | 1 | | | |
| | Authorised money changers | | | | 1 | 2 | | | | |

709. Overall, given the size of the Indian financial system and the approach to sanctioning, which can focus on individual transaction failings, the number of financial sanctions appears to be very low in general. Moreover, the actual level of the fines imposed (which appears to range on average between USD 10 000 and USD 20 000 for the banking sector) cannot be regarded as proportionate or dissuasive, especially given that some of these penalties appear to have been applied for systemic failures by the institutions. It should also be noted that the RBI has not yet imposed any sanction with regard to RRBs, StCBs and DCCBs, for which the NABARD can make recommendations based on its findings during the inspection of these institutions, and that; equally, the NHB has not imposed any sanctions to date.

Securities sector

710. Detailed provisions relating to penalties for failure to comply with all circulars issued under section 11 of the SEBI Act, including those related to AML/CFT compliance, are contained in section 15

⁶⁴ The term “agency” refers to a branch or other office of a licensed institution.

of the SEBI Act. The penalty that is to be imposed for any such violation is determined by an adjudicating officer through an inquiry that is detailed in sections 15I-15JA of the Act. This is without prejudice to actions that may simultaneously be initiated under the SEBI (Intermediaries) Regulations. Under Regulation 27, SEBI can take the following actions in cases where it has identified serious shortcomings during an inspection of a registered intermediary: (a) suspension of the certificate of registration for a specified period; (b) cancellation of the certificate of registration; (c) prohibition to take up any new assignment or contract or launch a new scheme for the period specified in the order; (d) prohibition of a principal officer from being employed or associated with any registered intermediary or other registered person for the period specified in the order; (e) prohibition of a branch or an office from carrying out activities for the specified period; and (f) a warning.

711. A decision to initiate proceedings under section 15 of the SEBI Act for imposition of a monetary penalty, or under the SEBI (Intermediaries) Regulations for action as provided under Regulation 27, is based on an assessment of factors, such as the gravity and nature of violation, likely impact on investors' interest, or the repetitive nature of the default. The actions include filing complaints for initiating prosecution under section 24 of the SEBI Act. There is no bar on initiating multiple proceedings wherever the nature of the case so warrants. The authorities provided a number of examples to illustrate that multiple proceedings are permissible and are taking place.

712. Under section 24 of the SEBI Act, SEBI also has powers to initiate prosecutions in cases of contravention of the provisions of the SEBI Act or of any Rules or Regulations issued there under. Sanctions may include a term of imprisonment, which may extend to ten years, or a fine, which may extend to INR 250 million (USD 5 million), or both. The procedure to determine whether the route of an administrative sanction or a criminal sanction originates with the division which carries out the inspection or investigation and prepares a course of action based on its findings. Usually, advisories or warnings would be issued in respect of less serious violations and the more serious cases would be referred to adjudication, enquiry or criminal prosecution depending upon the gravity of the violations and their impact on investors' interest and market integrity. The course of action is discussed internally in the Committee of Division Chiefs and an assessment of all the factors having a bearing on the case, is done at this stage. The recommendations are then put forward for the approval of the competent authority (Chairman/Whole Time Member of the Board) for action to be initiated in the case. It does not depend on SEBI to decide upon application of a criminal fine since the decision is of the Court. If the course of action approved is adjudication (for imposition of monetary penalty), an officer not below the rank of Division Chief is appointed as Adjudication Officer. The Adjudication Officer conducts the proceedings in line with SEBI (Procedure for Holding Inquiry and Imposing Penalties by Adjudicating Officer) Rules, 1995. As per section 15J of the SEBI Act and Rule 5(2), the following factors are to be considered by the Adjudication Officer while imposing penalty:

- a. the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default;
- b. the amount of loss caused to an investor or group of investors as a result of the default; and
- c. the repetitive nature of the default.

713. There is a Securities Appellate Tribunal (SAT) that has the authority to hear persons aggrieved by decision of SEBI. The next appellate level is the Supreme Court of India. The SAT looks at cases brought before it from the perspective of possible denial of natural justice and also the application of mind by the competent authority of SEBI that passed impugned Orders.

714. In the scheme of distribution of functions between the SEBI and the SROs, the primary responsibility for inspection and monitoring lies with the SROs. Stock exchanges and depositories are

empowered to take action against stock brokers and depository participants under their respective by-laws and regulations. The legal validity of these bye-laws and rules stems from sections 4 and 9 of the Securities Contract Regulation Act (SCRA), 1956 which permits an exchange to make by-laws for the regulation and control of contracts subject to the approval of SEBI, and grants recognition to an exchange if the by-laws conform to conditions of the SEBI. Various rules of the respective exchanges specify the disciplinary actions that can be taken by NSE and BSE against their members. These include expelling, suspending, fining, censure, warnings, and withdrawing any of the membership rights of members if they are guilty of a contravention, non-compliance, disobedience, disregard or evasion of any rules, bye-laws and regulations of the Exchange or any resolutions, orders, notices, directions or decisions or rulings of the Exchange. Similar wordings are in each of the rules of the stock exchanges.

715. In 2004, the exchanges also set up a points system in order to give weight to the history of actions taken against their members for repeated offences. For violations detected during the course of surveillance and investigation actions, penalty points are logged against the trading members based on the penalty norms approved by the Disciplinary Action Committee. The successive thresholds of the penalty point system lead to higher monetary penalties being levied. The exchanges have focused on an institution's history of violations and this is considered in the scheduling of inspections of the members. In this regard the two measures introduced recently (*i.e.* half yearly mandatory internal audit to be conducted by each member from August 2008 and the 100% annual coverage of brokerages through exchange inspection) cause the inspection regime between SEBI and the exchanges to focus on high risk areas.

716. The depositories (both the National Securities Depositories Limited (NSDL) and CDSL) are empowered to take disciplinary actions (including the imposition of fines) against their respective DPs for violations of their by-laws, rules, regulations. In this regard section 26 of the Depositories Act, 1996 (read with Regulation 3 of the SEBI (Depositories and Participants) Regulations, 1996) mandates the depositories to make by-laws with the previous approval of SEBI.

Application of sanctions by the SEBI and the SROs

717. At the time of the on-site visit, the SEBI had not applied any sanctions for purely AML/CFT violations, although it had dealt with cases where the underlying offence involved failures in CDD and other matters relevant to AML/CFT. On the other hand, the two stock exchanges, which provide the first line of regulatory defence in the securities sector, have applied a number of monetary penalties specifically for failures in AML/CFT systems. The NSE reported that the most common deficiencies related to failures by institutions to implement properly their written procedures, but that there appeared to be no common systemic failures in the sector.

718. The sanctions applied by SEBI for broader violations which include KYC/AML deficiencies (mostly CDD failures), are presented in the table below.

Table: General sanctions applied by SEBI including sanctions for AML/CFT

| Regulatory action | 2005 | 2006 | 2007 | 2008 | 2009 |
|--|------------|------------|------------|-------------|------------|
| Cancellation | - | 2 | - | - | - |
| Suspension | 8 | 23 | 13 | 3 | 2 |
| Warning | 9 | 7 | - | 1 | 2 |
| Censure | 7 | 10 | 6 | 1 | - |
| DPs directed not to open fresh dematerialised accounts | - | 13 | 1 | - | - |
| Total | 24 | 55 | 20 | 5 | 4 |
| Monetary penalties | | | | | |
| Adjudicating Officer Orders (value – INR mn) | 6 (1.4) | 8 (1.9) | 6 (0.6) | 1 (1.0) | 8 (2.2) |
| Consent Orders (value – INR mn) | | | | 5 (0.75) | 3 (1.4) |

719. In some of the cases mentioned in the table above, SEBI has imposed sanctions where purely AML/CFT violations were observed, as shown in the table below:

| Description | No. of entities | Sanction (in INR) | Details |
|--|-----------------|--------------------------------------|--|
| Settlement amount in case of DPs for violation of KYC Procedures | 8 | INR 2 150 000 | 6 Settlement Proceedings during 2008-09 and 2 in 09-10 |
| 11B order against DPs restraining them | 14 | Debarred from opening fresh accounts | 13 in 2006 and 1 in 2007 which continued till final penalty in 2008/2009 |
| Adjudication against DP | 1 | INR 100 000 | Paid in 2006 |

720. In respect of inspections carried out by the exchanges, sanctions for default are imposed by the exchanges themselves (see following table). In case of joint inspections, cases are referred to SEBI so that a decision may be taken on whether enforcement action should be taken jointly, severally or concurrently, all of which are possible under the various regulations. However, in cases emanating from joint inspections, action is usually taken by SEBI though exchanges are not prevented from initiating proceedings depending upon the nature, gravity and seriousness of violations. Hence, depending upon the nature of the violations detected, SEBI as well as stock exchanges may take necessary action based on their authority derived from respective by-laws or regulations.

Tables: Details of general inspections of stockbrokers conducted by the exchanges (NSE and BSE) and action taken with respect to AML/CFT deficiencies⁶⁵

| NSE | Year ending 31.03.2007 | Year ending 31.03.2008 | Year ending 31.03.2009 | Nine months to 31.12.2009 |
|---|-----------------------------------|-----------------------------------|-----------------------------------|--------------------------------------|
| No. of inspections | 371 | 239 | 282 | 430 |
| No. of cases where AML violations were observed | 113 | 25 | 20 | 158 |
| No. of cases where action taken | - | - | - | - |
| Advice issued | 112 | 20 | 6 | 154 |
| Fines levied | 1 | 5 | 13 | 4 |
| Value of fines imposed | INR 10 000 (USD 200) | INR 50 000 (USD 1,000) | INR 130 000 (USD 2,600) | INR 40000 (USD 800) |

| BSE | Year ending 31.03.2007 | Year ending 31.03.2008 | Year ending 31.03.2009 | Nine months to 31.12.2009 |
|--|-----------------------------------|-----------------------------------|-----------------------------------|--------------------------------------|
| No. of inspections | 271 | 297 | 176 | 191 |
| No. of cases where AML-violations observed | - | 2 | 23 | 9 |
| No. of cases where action taken | - | - | - | - |
| Advice issued | | 2 | 20 | 6 |
| Fine levied | | 0 | 3 | 3 |
| Value of fines imposed | | | INR 30 000 (USD 600) | INR 30 000 (USD 600) |

721. Similarly, the depositories have imposed a number of sanctions on their participants for failure to comply with the AML framework. For example, since the implementation of the PMLA in July 2005, has imposed monetary penalties of INR 3.14 million (USD 62 880) in 310 cases and CDSL has imposed monetary penalties of INR 3.4mn (USD67560) in 511 cases during the same period.

722. Although the number of sanctions applied in the securities sector appears to be relatively high, the value of the monetary penalties cannot be described as proportionate or dissuasive, with fines of as little as USD 200 equivalent per violation being applied. Violations can accumulate negative points for a broker as described above, and this is maintained by the exchange. SEBI has broad sanctions such as cancellations/suspensions/censure/regulatory warnings and debarment at its disposal, however the level of monetary penalties for most firms, would be seen as little more than an incidental cost of doing business.

⁶⁵ The term "Advice" is the lowest form of action taken by the relevant authority in respect of observations made during inspection wherein a trading member may be advised to ensure non-recurrence of the observations; ensure compliance with the relevant regulations of the Exchange; and put in place systems to rectify the violations observed.

In addition, there appears to be a marked discrepancy in the relative rate of AML/CFT deficiencies being identified by the NSE and the BSE. In the case of the NSE, 1 322 inspections carried out since 2007 identified 316 deficiencies, while the corresponding figures for the BSE are 34 deficiencies in 935 inspections. There is no reason to believe that the participants in the BSE should be any more attuned to their AML/CFT obligations than those in the NSE. India has attributed this to the possibility that BSE was the first and oldest exchange in Asia and was, until recently, an Association of Persons, whereas NSE has taken only corporate members on board. The number of single owner firms at BSE is very high and several of them do not deal for clients.

Insurance sector

723. Under section 14 of the IRDA Act, the IRDA has the general power to modify, withdraw, suspend or cancel the certificate of registration, although the IRDA Act does not specify the circumstances under which such action may be taken. However, section 3 of the Insurance Act further empowers the IRDA to issue, renew, suspend or cancel the registration. Powers to cancel the registration of an insurer can be exercised either wholly or in so far as it relates to a particular class of insurance business, for non-compliances with the stipulations on mandatory deposits, solvency margin requirements, insolvency, contravention of the legislation, directions or orders of the Authority, carrying on business activities other than the insurance business, etc.

724. The IRDA is also empowered under sections 102, 103 and 104 of the Insurance Act to impose monetary sanctions on insurance companies that fail to comply with the directions of the Authority, supply false information to the IRDA or fail to comply with investment regulations. These sections provide for penalties of up to INR 500 000 (USD 10 000) for each failure. Further the IRDA is empowered, under section 105, to impose sanctions directly on the management of Insurance Companies for offences committed by the company, and may initiate prosecution proceedings which render the person liable for criminal action under sections 102 (punishable with a fine) and 103 (punishable with a fine or imprisonment of up to three years). With respect to Intermediaries, section 42D(6) of the Insurance Act empowers the authority to cancel the licence of an intermediary or insurance intermediary for knowingly contravening any provision of the Act. The regulations to the Act further provide for rights to inspect, investigate and/or cancel or suspend a licence.

725. The process of initiating a penalty (on the basis of the experience in non-AML/CFT matters) originates with the official looking into a particular violation or non-compliance based on the findings of the on-site or off-site monitoring process. The proposal is then escalated through the entire hierarchy (3-5 levels based on the placement of the officer in the hierarchy who initiates the process). Ultimately the IRDA Chairman is the competent authority to decide upon the penalty, based on the nature of offence, recurrence of the violation, and the extent of loss to the policyholder. Currently, the legislation does not provide for a statutory adjudicating authority. Notwithstanding the initiation of any administrative proceedings, the IRDA may also decide to seek the imposition of criminal fines by the competent court (a Judicial First Class Magistrate). There is no statutory bar to concurrent administrative and criminal proceedings.

Application of sanctions by the IRDA

726. At the time of the on-site visit, no formal sanctions had been imposed, but advisories and show cause notices have been issued for non-compliance with the AML/CFT obligations in the IRDA's circulars, as indicated in the table below.

Table: Sanctions and Advisories issued to insurers/brokers/corporate agents for AML/CFT failures

| | No. of institutions regulated | No. of on-site examinations | Advisories | Monetary Penalties | Cancellation/suspension of licence |
|-----------|-------------------------------|-----------------------------|------------|--------------------|------------------------------------|
| 2006/2007 | 29 | - | | - | - |
| 2007/2008 | 31 | 16 | 16 | - | - |
| 2008/2009 | 36 | 33 | 2 | - | - |
| 2009/2010 | 43 | 6 | 1 | - | - |

727. Advisories issued are not necessarily related to on-site inspections, for example, during the financial year 2007-2008 advisories related to focussed inspections carried out in May 2007 and during 2008-2009, advisories were based on off-site monitoring and not on the on-site inspections indicated above. As with the other regulatory authorities, there is no evidence that the sanctioning regime is effective, proportionate and dissuasive in the insurance sector.

Market Entry – Recommendation 23

Reserve Bank of India (RBI)

728. All institutions engaged in banking business must be licensed and supervised by the RBI in accordance with the Banking Regulation Act. The granting of a licence is subject to fulfilment of a range of conditions, including both financial and good governance tests. Licensing and structure provisions of banking companies are contained in sections 21(1) and 21(3)(d) of the Banking Regulation Act, although no new banking licences have been issued since 2001, on the basis of a government policy to restrict further access to the market for the time being. The authorities have indicated that, in the event that this policy is reviewed at some time in the future, detailed criteria for establishing a new bank will be established.

729. There is no explicit statutory power for the RBI to halt the acquisition of shares by undesirable persons or to remove the voting powers of any person deemed not to be fit and proper. However, through various circulars issued between 2002 and 2004, banks were advised that the acquisition of shares of five percent and more of the paid-up capital of a private sector bank by an individual or group requires the prior acknowledgement of the RBI. Private sector banks were advised to amend their Articles of Association in order to enforce this requirement on the shareholders and management. The RBI does not consider this instruction to be *ultra vires* in the light of the principles laid down by case law⁶⁶. Since January 2007, the RBI has refused three requests to acquire 5% or more of the paid up capital of a bank without any apparent difficulty in enforcing the terms of the control.

730. The Banking Regulation Act has certain built-in safeguards to protect the interest of regulated entities, as major actions under the Act are either taken in consultation with the Central Government or are appealable. Certain sections of the Banking Regulation Act specifically provide for appeals to Central Government (e.g. section 22 provides for appeal against cancellation of a banking licence, and sections 10B and 36AA provide for appeals against an RBI order for removal of Chairman or Managing Director or others of a bank). In case an application for banking licence is rejected by RBI, there is no Appellate Authority to which an appeal against the decision of the RBI can be filed, although, decisions of the RBI in the matter can be challenged in a court of law. However, there has not been any case where application for banking licence was rejected by RBI but allowed on appeal.

⁶⁶ Bank of India Finance Ltd vs. *Custodian*.

731. The licensing or registration of the different entities regulated by the RBI is done by the various regulatory departments under the relevant statutory powers. Licensing of commercial banks as well as of urban co-operative banks and non banking finance companies is undertaken at the RBI Central Office and licensing of rural co-operative structure is done at 26 Regional Offices in various provinces and states. The Regional Offices operate as extended arms of the respective Central Office Departments, and each Regional Office has a defined jurisdiction over entities situated in the defined geographical jurisdiction.

732. In terms of the “fit and proper” criterion for persons associated with the institution, the Banking Regulation Act focuses exclusively on the management. Section 22(3)(c) requires that “the general character of the proposed management of the company will not be prejudicial to the public interest or the interest of its depositors”, while section 10A requires that the Board of Directors includes persons with specific professional experience. Directors of the public sector banks and the RBI subsidiaries are appointed directly by the Government of India, together with RBI-nominated directors. RBI Nominee Directors in private sector banks are appointed by the RBI “as when needed” under section 36AB of the Banking Regulation Act. The full-time directors of private sector banks may be appointed only after prior approval of the RBI under section 35B of the Banking Regulation Act. Section 35B(b) also requires that any appointment or re-appointment or termination of appointment of a chairman, a managing or full-time director, manager or chief executive officer or similar requires prior approval of the RBI. While there are no specific provisions relating to the integrity of the management, the RBI issued guidance to this effect—described below. Section 36AA gives the RBI the power to remove from office any person involved with the management of a bank (from the Chairman down) if it believes it would be in the public interest to secure the proper management of the bank.

733. In addition to the requirements under the Banking Regulation Act, the RBI has issued several circulars with “fit and proper” requirements for the management of the institutions it licenses, but these are directed at the procedures that banks are expected to implement when appointing senior personnel. For example, the appointment of part-time non-executive directors in private sector banks is carried out by the banks themselves after carrying out due diligence for ‘fit and proper’ status, as stipulated in the RBI circular of 25 June 2004, which provides for broad guidelines, including integrity. This is the responsibility of the Nomination Committees of the banks themselves. The Committees are however advised in the guidelines (1 June 2007) that criteria must include experience, expertise and integrity. The RBI asserts that during inspections, if it becomes aware that the candidate(s) does not meet the fit and proper criteria, it has the right to remove the said non-executive director. There have been cases (dated 2004 and 2008) where the RBI has initiated action by issuing a Show Cause notice under section 36AA(2) of the Banking Regulation Act, which empowers it to remove any Chairman, Director, Chief Executive Officer from office for non-adherence to its “fit and proper” guidelines. However, according to the FATF standards, such scrutiny should take place prior to appointments of management by the supervisor rather than in retrospect.

734. A declaration form with more details and questions on, amongst other criteria, disciplinary hearings/criminal prosecution/convictions and if the director had at any time received an adverse notice from regulators, has to be signed by all elected directors. All the elected directors execute the deeds of covenants as recommended in the Circular dated 20 June 2002 that provide recommendations for the Board of Directors that while nominating and co-opting directors, they should be guided by certain criteria like criminal records, civil actions admission/expulsion from professional bodies and sanctions by regulators and other bodies. It is also mandatory that all elected directors furnish a declaration every year as on 31 March that the information already provided has not undergone any change and where there is any change requisite details are furnished. If there are significant changes, the Nomination Committee should undertake due diligence afresh and subject the candidature to the ‘fit and proper’ test. The NABARD has issued guidelines on criteria for selection of the Chairman of a RRB and, section 12 of the RRB Act states

that a person shall be disqualified for being appointed or nominated as a Director, if he is or has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude.

735. NBFCs are issued a Certificate of Registration under section 45IA of the RBI Act, which has a similar provision to that in the Banking Regulation Act, in that the RBI must be satisfied that the character of the management will not be prejudicial to the interests of the depositors. At the time of registration, the fit and proper test of the directors of the applicant company is carried out based on the declaration that is given by each new director in Annex-III to the application form. Any change in the management/director of a company that has received registration from the RBI is to be communicated to RBI within 30 days of the change in management/director. The NHB has a similar provision as for the NBFCs, under Chapter V of the NHB Act, which says that the NHB must be satisfied with that the character of the management will not be prejudicial to the public interest or interest of depositors. The NHB Act is silent on any declaration of a change in management in the deposit-taking institution to be made to the NHB, however, in February 2010, the NHB issued directions that require prior approval in writing from NHB for the acquisition or transfer of control (control defined in the similar vein as the SEBI regulations) of deposit-taking housing finance companies.

736. Money service businesses and foreign exchange houses are licensed by the RBI under the FEMA, section 10(1) but are not subject to prudential supervision under this legislation. The FEMA is silent on the conditions under which a licence may be issued, and does not address the probity or character of shareholders. However, under sections 10(4) and 11(1) of the FEMA, the Reserve Bank issued guidelines to Authorised Money Changers on 9 March 2009, which contains details of the eligibility norms for licensing. Amongst several other criteria, a declaration is required to the effect that no proceedings have been initiated by or are pending with the Directorate of Enforcement or the Directorate of Revenue Intelligence or any other law enforcement agencies against the applicant company and its directors, and that no criminal cases have been initiated or are pending against the applicant company and its directors. The circular also contains instructions to the AMCs about the procedures to be adopted by the governing board when appointing new directors. The circular specifies that appointments should be based on qualification, expertise, track record, integrity and other 'fit and proper' criteria, and it goes on to explain how these tests might be applied. However, the regulatory authority is not involved in this process.

Securities and Exchange Board of India

737. Chapter V, read with section 12, of the SEBI Act provides for mandatory registration of stock brokers, sub-brokers, merchant bankers, depository participants, foreign institutional investors⁶⁷ and other intermediaries who may be associated with the securities market. Chapter and Schedule II of the SEBI (Intermediaries) Regulations provide for detailed norms for registration of intermediaries and provide that the Board "may" take into account any criteria it deems fit, including but not limited to the following:

- a. integrity, reputation and character;
- b. absence of convictions and restraint orders;
- c. competence, including financial solvency and net worth.

Furthermore, the regulations automatically debar anyone from continuing in office if they are convicted of economic crimes, fraud or dishonesty.

⁶⁷ Apart from the investments by natural and legal persons based in the country, money from abroad enters the capital markets through the vehicle of Foreign Institutional Investors (FII) that are registered by SEBI prior to their entry in the market. FIIs may be non-residents of India.

738. There are no equivalent provisions relating to shareholders in the primary legislation. The Regulations lay down the registration process (Regulation 5 of Chapter II of the SEBI Stockbroker Regulations, 1992) and define a mandatory obligation of the Board with respect to the application of fit and proper criteria to each key management person. Further, under regulation 6A(1)(c), any change in ownership and change in control in an intermediary requires prior approval of SEBI without any exemption. In order to clarify the term ‘change in status and constitution’, SEBI issued a circular on 9 July, 2003, in which it was stipulated that the following would be the circumstances that would require the prior approval of the SEBI:

- a. change in designated or full-time directors who are generally responsible and accountable for the affairs of stockbrokers, but this does not apply to “ordinary directors”⁶⁸ for whom prior approval is not required by SEBI. However, Fit and Proper Criteria” apply to all directors whether ordinary or designated. In the case of ordinary directors, approval by the stock exchanges is mandatory in all cases, and this includes fit and proper due diligence. In case of designated directors, as an additional measure, prior approval of SEBI is also required. The purpose of designating a minimum of two such directors is to provide comfort to the regulator about the necessary expertise and accountability in functioning of the stock broker.
- b. change in ‘control’, which would have the same meaning as defined in the SEBI (Substantial Acquisition of Shares and Takeovers) Regulations, 1997⁶⁹.
- c. conversion from one form to another (proprietorship, partnership and corporate);
- d. transfer by way of sale, nomination, or otherwise;
- e. consolidation, merger or amalgamation of brokers;
- f. surrender of certificate of registration.

739. Only applicants who have been offered membership of the exchange are eligible to be registered with SEBI. Exchanges only admit members who fulfil their own eligibility criteria and the criteria defined by SEBI. All the compliance requirements of the SEBI regulations (including the “fit and proper person” test) have been incorporated into by-laws, regulations and rules of the exchanges. As regards registration of sub-brokers, exchanges receive all the registration documents through the trading members. Based on the records submitted, trading members recommend the applicant to be registered as sub-broker of the main stock broker and send all the documents to SEBI, which, after carrying out its validations, grants registration to sub-brokers.

740. In the event that an application for registration is refused, SEBI must communicate its decision within thirty days to both the applicant and the relevant exchange. Thereafter, the applicant has the right of appeal. SEBI has not rejected any applications in the past three years, having issued some 756 certificates of registration over that period. However, since all applications are processed initially by the exchanges, the exchanges become the first line of defence against undesirable entrants to the market. While the NSE

⁶⁸ Ordinary (non-designated) Directors are part of the Board of Directors of the Company and the Board is vested with powers to manage the affairs of the Company within the powers defined under the Companies Act.

⁶⁹ The Regulations define 15% or more as a significant threshold in ownership or control through a PAC or control through ability to appoint directors on the Board. “Control” shall include the right to appoint the majority of the directors or to control the management or policy decisions exercisable by a person or persons acting individually or in concert, directly or indirectly, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements or in any other manner.

reported that it had not rejected any applications over the same three-year period, the BSE had turned down 20 approaches, mostly on the grounds that the applicants failed to make the required deposit.

741. Similar procedures are followed with respect to the depository participants. Applications for registration are lodged initially with the depository, which then forwards its recommendation to SEBI. The Regulations empower the depository to set its own selection criteria in its by-laws. In the case of the CDSL, for instance, these include requirements that:

- a. the applicant should not have been convicted in any of the five years immediately preceding the filing of the application in any manner involving misappropriation of funds and securities, theft, embezzlement of funds, fraudulent conversion or forgery;
- b. the applicant should not have been expelled, barred or suspended by SEBI, a self regulatory organisation or any stock exchange, provided that, if a period of three years or more has elapsed since such punishment was imposed, the Depository may, in its discretion consider such application.
- c. the applicant shall be required to furnish information and details of his business history including the background and experience of directors and promoters of the applicant.

742. The two depositories have processed 210 applications in the past three years, of which five were deferred and two rejected. The two rejections related to failure to meet the technical admissions criteria, rather than concerns about the ability to meet the “fit and proper” criteria.

Insurance Regulatory Development Authority

743. Registration as an insurance company is governed by the Insurance Act, and the registration criteria are set out in the IRDA (Registration of Indian Insurance Companies) Regulations, 2000. Before issuing a registration certificate, the IRDA is required, under the Regulations, to consider, amongst other things,

- a. the record of performance of each of the promoters in the fields of the business or profession in which they are engaged;
- b. the record of performance of the directors and persons in management of the promoters and the applicant;
- c. the level of actuarial and other professional expertise within the management of the company; and
- d. the financial condition and general character of management of the applicant.

The IRDA processes applications through a centralised desk, which undertakes due diligence checks. These checks, which may involve enquiries with other domestic or foreign agencies, are routed through a screening committee that comprises members of the various IRDA departments.

744. Regulation 13 provides that, in the event that an applicant is aggrieved at any decision to reject the application, he may appeal to the Central Government to reconsider the matter. To date, the appeal process has never been used because the IRDA has not rejected any applications, of which ten have been approved over the past three years.

745. Under section 6A(4)(b)(ii) of the Insurance Act, any transfer of shares that results in a holding of five percent or more of the ownership of an insurer requires the prior approval of the IRDA. The threshold is reduced to two and a half percent where the holder is either a bank or an investment company. Sub-section (4)(b)(iii) goes on to state that prior approval is also required “where the nominal value of the

shares intended to be transferred by any individual, firm, group, constituents of a group, or body corporate under the same management, jointly or severally exceeds one per cent of the paid-up equity capital of the insurer”. As part of the compliance process, insurers are required to file a quarterly return showing the shareholding pattern.

746. The appointment of a full-time director, managing director or chief executive officer is governed by the provisions of section 34A of the Insurance Act. This requires that “no amendment made of any provision relating to the appointment, re-appointment, termination of appointment or remuneration” of such persons shall have effect unless approved by the IRDA. Section 34B provides the IRDA with the authority to require the removal of any director or chief executive officer when it considers the action to be in the public interest; to prevent the affairs of the insurer being conducted in a manner contrary to the interests of the policy-holders; or to secure the proper management of the insurer.

Ongoing supervision and monitoring – Recommendation 23

Reserve Bank of India (RBI)

747. Banking companies are subjected to ongoing supervision based on section 35 of the Banking Regulation Act. Inspections concentrate on core assessments based on the CAMELS model, which addresses capital adequacy, asset quality, management, earnings, liquidity and systems and controls. The RBI has developed a risk-based model of supervision that aims not only to allocate supervisory resources more effectively, but also places greater emphasis upon risk management within institutions. During the inspections of banks, the RBI also looks into compliance by banks with the instructions issued through the different AML/CFT circulars. There is no separate AML/CFT inspection programme, since the prudential inspections contain an AML/CFT component, which is carried out by the regular RBI inspection teams.

748. The RBI has its Central Office located at Mumbai and 26 regional offices in various provinces and states. Staff in the regional offices operates as an extended arm of the respective Central Office departments. Each regional office has supervisory jurisdiction over entities situated in a defined geographical area. In order to ensure consistency in policy at institutional level, the Central Office of each department formulates the policy framework, and the regional offices ensure compliance by the respective regulated entities under their jurisdiction. Therefore, supervision of all types of entity is undertaken by the regional offices under the overall guidance of the Central Office, which has laid down prescribed criteria for the selection of branches of regulated entities that should be inspected.

749. For inspections conducted prior to 1 April, 2009, the regional offices were required to select branches for inspection in such a way that at least 30% of the total advances for Indian banks (both private and public sector) and at least 60% of the advances for foreign banks operating in India are covered every year. To achieve this, annual inspections are required of all branches involved in operations relating to treasury, corporate finance, international finance, stock exchange/clearing, central processing and strategic business, as well those deemed to be exceptionally large, high risk or prone to fraud. Very large branches, 1% of rural branches and a mix of large, medium and small branches are required to be inspected on rotation basis.

750. However, the RBI policy has since been modified given the changes that have taken place in the business processes adopted by banks, such as the setting up of centralised or regional asset/liability processing centres; the centralized processing and monitoring of large corporate loans, and the introduction of core banking solutions. The new policy maintains many of the previous fixed criteria, but adds a range of risk factors, such as the relative importance and scale of the operations, the exposure to different sectors and products deemed to pose particular risks, and high growth rates in either advances or deposits. However, it is no clear from this model the extent to which AML/CFT risk is taken into account (beyond

being captured within the category of “prone to fraud”), given that AML/CFT compliance is subsumed within the general inspection process, rather than being treated separately.

751. In some instances, at least, the regional offices have been given specific instructions on AML/CFT compliance procedures. For example, with respect to the urban co-operative banks, the regional offices were advised through circulars issued by the Central Office in September 2007 and February 2009 that the inspection officers should comment on the compliance of UCBs with KYC/AML guidelines; examine the systems in place in the banks for timely submission of CTRs and STRs, and comment on their adequacy; and assess the role of the Principal Officer. The RBI’s regional offices have also been specifically instructed to assess the effectiveness of the system in place in the UCBs for circulation and dissemination of lists of designated terrorist individuals/entities to their branches. It is unclear the extent to which this approach has been adopted by other supervisory departments, and whether these procedures are to be applied in conjunction with the standard inspection framework, or whether they create a separate model purely for AML/CFT.

752. The Department of Banking Supervision’s (DBS) inspection manual, designed for prudential supervision, contains a separate “chapter” on AML/CFT examination. The DBS also issued a letter in 2008 advising all Regional Officers that inspection reports should “invariable contain specific comments on compliance” with the guidelines on AML/CFT, including CTRs, STRs, maintenance of customer profile, adoption of technology, etc. However, the assessment team is of the view that the “chapter” in the inspection manual includes a checklist rather than detailed instructions focusing on specific high-risk areas, etc. This finding raises a concern with regard to effectiveness, specifically in relation to the scope and the adequacy of the RBI’s current AML/CFT inspection process.

753. The FIU-IND is actively involved in training the supervisors to understand the factors listed in the RBI checklist to verify the effectiveness of each component of the AML/CFT system and processes. The Indian authorities also report that the RBI regularly obtains input related to ML/FT risks from various sources such as the FIU-IND (compliance history of the bank, STRs involving systemic issues), the Central Economic Intelligence Council (crime trends, modus operandi, high risk products and risks), the Regional Economic Intelligence Council (regional trends and modus operandi) and other law enforcement and intelligence agencies. The Indian authorities explained that the information received from the different intelligence sources is used by the inspection teams to prepare for a more focused inspection.

754. Inspections by the RBI’s DBS cover both the head office and selected branches of banks. The RBI explained that at the head office level, inspections focus on systemic issues while at the branch level, inspections focus at the transactional level. The branch inspection reports are in narrative form and feed into the head office report. If during the inspection of a bank large scale irregularities related to any specific area, including AML/CFT is noticed, the RBI may decide that such a situation warrants a system-wide examination.

755. In addition, the RBI undertakes “Special Inspections” focusing specifically on KYC/AML issues. The RBI explained that this kind of inspection is basically targeted at the books of accounts and related documents of specific account holders against whom a complaint has been received, or who have been found to have indulged in fraudulent activities. These inspections are mainly triggered by external inputs mentioned above. They are basically pointed towards verification of KYC documents and the CDD procedures followed by the bank in relation to specific accounts. However, the assessment team is of the view that these special inspections cannot be considered as thematic AML/CFT inspections.

756. The following table gives an overview of the special inspections the RBI has undertaken in the period covering the years 2007-2009:

| Year | Number of special inspections |
|------|-------------------------------|
| 2007 | 77 |
| 2008 | 87 |
| 2009 | 92 |

757. The findings of all inspections are conveyed to the bank, which is required to report back on the shortcomings identified. If the RBI considers that the comments and reactions provided are not satisfactory, it will issue a Show Cause Notice and will call on the bank to provide arguments, including via a personal hearing of the bank's CEO, why the RBI should not impose a penalty or take any other supervisory action.

758. In February 2009, the RBI instructed the NABARD to focus its supervisory efforts on the assessment of compliance with the RBI AML/CFT circulars for RRBs, StCBs and DCCBs. Based on its inspection findings, NABARD makes recommendations to the RBI for regulatory actions to be taken, wherever required, under the provisions of the Banking Regulation Act. Similar procedures are employed by the NHB. As indicated above, to date, no penalty has been imposed for AML/CFT violations by any institution under the supervision of either the NABARD or the NHB.

759. Authorised money changers, money remittance companies, and Indian Agents under the Money Transfer Services Scheme (MTSS) are subject, *inter alia*, to transaction reporting requirements, which involves a monthly return on sale and purchase of foreign currency notes for the Authorised Money Changers, and a quarterly return on remittances received for the money remitters and Indian Agents under the MTSS. They are inspected by the RBI or NABARD for compliance with the FEMA regulations, which include AML/CFT and record-keeping requirements. In addition, based on the reporting statements, the RBI also undertakes off-site monitoring of the authorised money changers and the money remitters.

760. The following table lists the total number of inspections carried out by the RBI over the period 2006-2009. As indicated above, the inspection programme does not involve specific AML/CFT visits, but compliance with the PML Rules and the RBI circulars forms part of the routine inspection procedures. The Department of Banking Supervision (DBS) has advised Regional Offices in a Circular dated 2 November 2006 to examine/ascertain the extent of actual compliance by banks to their KYC/AML obligations as per the guidelines issued and as such every annual financial inspection contains as AML/CFT component. More recently, the DBS issued a Circular dated 8 September 2008 advising Regional Offices to ensure that the All Financial Institutions (AFI) reports invariably contain specific comments on compliance with guidelines by the bank on KYC/AML/CFT including the issues relating to cash transaction reports and suspicious transaction reports, maintenance of customer profiles, adoption of technology etc.

Table: General inspections (not specific to AML/CFT) carried out by the RBI (2006- 2009)

| Category of banks | Year 2006 | | Year 2007 | | Year 2008 | | 2009 (to June) | |
|------------------------------|--------------------------|-----------------------------|--------------------------|-----------------------------|--------------------------|-----------------------------|--------------------------|-----------------------------|
| | No of entities regulated | No of inspections conducted | No of entities regulated | No of inspections conducted | No of entities regulated | No of inspections conducted | No of entities regulated | No of inspections conducted |
| Scheduled Commercial Banks | 90 | 90 | 95 | 91 | 90 | 87 | 87 | 83 |
| Urban Banks | 1 839 | 1 213 | 1 785 | 1 213 | 1 740 | 1 276 | 1 714 | 424 |
| Co-operative and rural banks | 530 | 416 | 496 | 335 | 493 | 366 | 488 | 355 |
| Authorised money changers | 1 053 | - | 1 090 | - | 1 143 | 100 | 1 155 | 258 |
| | 544 | 92 | 516 | 41 | 537 | 98 | 543 | 75 |

Securities and Exchange Board of India (SEBI)

761. SEBI conducts inspections of intermediaries on an independent basis, although it is not the primary day-to-day inspection agency. This role is fulfilled by the exchanges (see below). SEBI will typically become involved when there are specific concerns about an institution, particularly in relation to possible offences under the securities legislation. In principle, the scope of the SEBI inspections covers the following AML/CFT aspects:

- a. appointment of Principal Officer and intimation to FIU-IND;
- b. formulation of AML Policy and its implementation;
- c. intimation of Client Identification Procedure to FIU-IND;
- d. categorisation of clients based on their Risk Profile;
- e. systems for generation of alerts, identification of Suspicious Transactions and reporting thereof, when necessary;
- f. checks to ascertain there were no cash transactions;
- g. maintenance of records;
- h. systems in place for screening of employees while hiring;
- i. adequate training to staff on AML and CFT; and
- j. an independent audit of AML policy.

762. SEBI considers various factors while short-listing intermediaries for inspection: the number and nature of any complaints; the number of defaults; and the turnover volume. In addition, inspections are conducted on the basis of referrals received from SEBI departments, external agencies, press reports, etc. Compliance with key features of the AML/CFT framework forms part of the SEBI inspection manual for

stock brokers. Inspection findings are discussed with the management of the entity on the last day of the inspection. Thereafter, inspection reports are prepared and, once approved, are sent to the broker for its comments, which are taken into account when finalising the report's recommended action. The Inspection Division of SEBI has recently taken an initiative to discuss the findings with the entity's management and compliance team. Entities are then given an opportunity to report back to SEBI about the corrective actions taken to improve their operations. SEBI's Committee of Internal Division Chiefs reviews the post-inspection analysis and the recommended action. If the observations are of a serious nature, have systemic irregularities, or raise concerns over the risk management, then additional follow-up inspections are conducted with any necessary expertise being drawn from other departments or the stock exchanges.

763. However, routine compliance monitoring is primarily exercised through the exchanges, which have been issued with policy directives by SEBI to conduct regular audit/inspections of stock brokers. With regard to AML/CFT, the stock exchanges have been advised to cover the following aspects:

| Important Parameters | Methodology |
|--|--|
| Customer acceptance policy and customer due diligence measures | What is the process adopted by member to verify the identity of the customer and/or the person on whose behalf a transaction is being conducted? |
| Walk through of the process | |
| Process of generation and monitoring alerts | |
| System in place that allows continuous monitoring of transactions | Whether any account was opened in fictitious name/benami account? |
| Process for identifying STRs and reporting the same to the FIU-IND | What checks and balances are in place to ensure that the identity of the client does not match with any person having criminal background or is not banned in any other manner? |
| Processes for verification of alerts with KYC details | |
| | What are the factors of Risk perception having regard to the client's location, address, nature of business activity, trading turnover and the manner of making payments so that the clients can be classified in to "High Risk", "Medium Risk", or "Low Risk" category? |
| | Whether details of appointment of Principal Officer and change in Principal officer, if any, is intimated to the FIU-IND? |
| | Whether member has adopted and implemented written AML procedures |
| | Whether member has adequate system to generate alerts for suspicious transactions? |
| | As per provisions of Prevention of Money Laundering Act, 2002 whether record of transactions, its nature and its value are maintained? |

764. With effect from the financial year 2009-2010, stock exchanges have been directed to inspect all its active members each year. Also, all trading members have been directed to have their operations audited on a half-yearly basis, to include checks on compliance with exchange by-laws and SEBI regulations. The scope of the exchange inspections includes examination of customer due diligence; books of accounts, records and documents; dealings with clients and intermediaries; risk management and AML compliance with respect to PMLA. Based on the inspection findings, a letter of observations and/or a "show cause notice" is issued for any violations identified. On receipt of the reply from the broker, the matter is placed before the Internal Committee for Minor Actions or the Disciplinary Action Committee. Trading members are given personal hearing, either at their request or on the decision of the Committee. Based on the written and oral submissions and documentation, the Committee decides on the action to be taken and issues a letter to that

effect, following which, compliance with the decision is verified during the next inspection. The relevant Committees consist of both outside experts and officers of the exchange who review the overall inspection findings, from time to time, to identify any systemic issues which may require additional guidance or cross-sectoral action. The findings of the inspections are also included in an inspection report that is provided to SEBI.

765. Joint inspections with SEBI are also carried out, especially when there are identified problems with a broker (although only two have been conducted in the past two years, but none involving AML/CFT issues⁷⁰), and SEBI holds a weekly meeting with the exchanges to discuss regulatory issues. SEBI also conducts inspections of the exchanges themselves, to help ensure that the regulatory framework is being properly implemented.

766. The following table shows the total number of inspections carried out by SEBI and the exchanges. These statistics do not relate solely to AML/CFT compliance monitoring, since this forms only one part of the overall examination. Pursuant to the enactment of the PMLA, the PML Rules and the issuance of regulatory circulars, compliance with AML/CFT obligations is an essential element for all inspections carried out by SEBI, the stock exchanges and the depositories. Compliance with various AML/CFT requirements has been included as an important part of the check list prepared for such inspections. Stock brokers and depository participants are subject to SEBI inspections, inspections by the stock exchanges/depositories and an independent internal audit which is conducted on a half-yearly basis purely from the compliance angle. This information is indicative of the frequency of inspections and the compliance culture in securities market.

General inspections (not specific to AML/CFT carried out by SEBI and the Exchanges)

| Examining body | 2006-2007 | | 2007-2008 | | 2008-2009 | | 9 months to 31.12.2009 | |
|----------------|--------------|-------------|--------------|-------------|--------------|-------------|------------------------|-------------|
| | institutions | inspections | institutions | inspections | institutions | inspections | institutions | inspections |
| SEBI | - | 67 | - | 63 | - | 38 | - | 49 |
| NSE | 959 | 371 | 1028 | 239 | 1094 | 282 | 1247 | 430 |
| BSE | 640 | 271 | 692 | 297 | 744 | 176 | 779 | 192 |

767. Additionally, the NSE and BSE jointly conduct limited purpose inspections of brokers with regard to AML/CFT compliance. These inspections (of which there were about 20 in 2008) focus on areas such as the appointment of a Principal Officer; in-person verification of clients; periodic review of client information; risk categorisation of clients; systems for monitoring suspicious transactions and generating alerts; ongoing AML training for employees; and implementation of written procedures. Based on the findings of these inspections, the exchanges issue advisory notices for improvement to their members.

⁷⁰

As a matter of practice, as individual exchanges cannot look beyond the transactions executed on their own trading platform, joint inspections are conducted in order to take an overall view on the complete functioning of the trading member across the various exchanges.

768. The depositories, which also act as *de facto* SROs, inspect their participants, who act as the direct point of contact with customers, and who are, therefore, responsible for undertaking CDD. The depositories' inspection powers derive from both statute and contract with the participants. They are required to inspect each participant every year, using a standard checklist of issues to be addressed. Limited scope inspections are also undertaken from time to time. The internal procedures for handling the output from the inspection programmes are similar to those used by the exchanges. Each depository has about 400 participants, of which about 150 are members of both. As with the exchanges and their members, SEBI also has the power to inspect both the depository and the participants.

Insurance Regulatory and Development Authority

769. Compliance with the AML/CFT guidelines by the insurance companies undergoes scrutiny by the IRDA, both off-site and on-site, as follows:

- a. Insurance companies are mandated to file their AML/CFT policies with the Authority before they commence their business operations and such policies are reviewed within 2-5 days of filing. Deficiencies or errors observed in the policy are notified to the insurance companies, and they are directed to bring about changes or modifications to their AML policies. Confirmation of compliance is sought on operational issues which lack explicit mention in the policy;
- b. the Inspection department undertakes focused and market conduct inspections involving compliance checks on AML guidelines. Focused inspections to check levels of implementation of the AML/CFT guidelines were undertaken in 2007. Following the inspections, the insurance companies are directed towards corrective or preventive actions based on the outcome of the inspection reports, after giving them an opportunity of being heard. On issues pertinent to the industry as a whole, circulars are issued for necessary action;
- c. the life insurance department pursues follow-up action on the findings of the market conduct inspections; and
- d. the actuarial department clears all the life insurance products which are required to be filed with the Authority as part of the "file and use" procedure⁷¹.

770. The IRDA uses an internally developed AML/CFT inspection manual, which broadly covers vulnerable areas in the insurance business, and covers the checks and controls laid down in the AML/CFT guidelines issued by the Authority. The manual also focuses on the areas and documents to be examined in order to ascertain that the appropriate systems and procedures in place. The number of examinations undertaken by the IRDA is shown in the following table.

Table: General inspections undertaken by the IRDA

| | No. of institutions regulated | No. of on-site examinations (AML/CFT issues) | No. of on-site examinations (other than AML/CFT issues) |
|-----------|-------------------------------|--|---|
| 2006/2007 | 29 | - | 8 |
| 2007/2008 | 31 | 16 | 13 |
| 2008/2009 | 36 | 33 | 17 |
| 2009/2010 | 43 | 6 | 14 |

⁷¹ The "file and use" procedure contains a checklist for collection of documents towards identity proof, residence proof, income proof, and photographs. Other documents required in relation to the underwriting norms of the insurance companies like age proof, customer's self declaration, etc. are also relevant in this context.

771. A specialist AML/CFT department within IRDA also conducts off-site monitoring of the sector through STRs disseminated to it by the FIU-IND. The STR related information received from the FIU-IND is analysed and, if necessary, further details are requested from the FIU-IND and/or the insurance company involved. This information is also used by IRDA to develop typologies for the sector. On the basis of the STRs received so far, two of the companies have been directed to review their processes as compliance with the AML/CFT guidelines was not observed. The shortcomings are also brought to the attention of the entire industry. In other cases, the STRs raised concerns on other than AML issues and they were forwarded the relevant departments of the Authority for further action.

Guidance for financial institutions (other than on STRs) - Recommendation 25

772. As described in detail above, the RBI, SEBI and IRDA have all issued detailed circulars to the regulated institutions to impose mandatory obligations but also to assist the institutions concerned in complying with their obligations under the PMLA. The guidelines broadly cover the following areas:

- a. AML policies, procedures and controls;
- b. KYC norms;
- c. reporting of transactions to the FIU-IND;
- d. appointment of a Principal officer;
- e. organisation of effective AML training for staff members;
- f. customer education;
- g. internal control/audit mechanisms as an AML control measure; and
- h. examples of suspicious transactions.

773. The RBI entrusted the Indian Banks' Association (IBA) with the task of preparing broad outlines of a policy framework with illustrative examples to serve as a reference guide to the banks. The first set of IBA guidelines was issued in 2005, when the PMLA came into force. The IBA updated the guidelines in July 2009 to include the developments in both India's AML/CFT legal framework and the typologies. In updating its guidance notes, the IBA has worked closely together with the FIU-IND.

774. In addition to the circulars issued by SEBI, the stock exchanges and the depositories have also issued guidelines, instructions and clarifications on the various aspects of AML/CFT. The guidelines provide for a broad AML/CFT policy framework which intermediaries should put in place, the possible scenarios of suspicious activity, the detailed requirements relating to CDD procedures, independent testing of AML/CFT systems and procedures, hiring standards and training needs, etc. In addition Association of Mutual Funds in India (AMFI) puts out regular guidance papers to the Asset Management Companies in relation to KYC, CDD and parameters for filing of STRs with the FIU.

775. In the insurance sector, the IRDA has organised various meetings/briefing sessions for officials of insurance companies. Officials of the FIU-IND provided input on the reporting requirements during such sessions. Insurance companies are also briefed on a one-to-one basis over the phone, by letters and e-mails, and during their personal visits to IRDA. IRDA frequently interacts with the FIU-IND to check compliance with the reporting requirements by the insurance companies.

776. Apart from specific guidance issued by the FIU with regard to reporting of STRs and CTRs (see section 3.7 above), the FIU-IND has also issued a general guidance paper on Obligations of Entities in the Financial Sector under the PMLA.

Implementation and Effectiveness

777. *Resources:* Generally, the RBI and SEBI appear to be well resourced, both in terms of budgetary funding and human resources. However, in the case of the RBI, the relatively large number of supervisory staff has to be set off against the scale, diversity and geographical distribution of the financial sector for which it is responsible. The SEBI is clearly a smaller, leaner organisation, but it has the relative advantage of supervising a smaller, more compact sector where technological developments and the supervisory role of the exchanges assist the process considerably. The position with respect to the IRDA is less clear-cut. While there are only 44 licensed insurers in India, they operate throughout the country through a branch and agency network, and their supervision is vested in a body with just 126 staff, including four AML/CFT specialists. The authorities admit the need to replenish human resources and efforts have been made, as recent as February 2010, to recruit 14 additional officers, some of whom are deployed specifically to the inspection department that reviews the compliance of AML/CFT guidelines. However, at this early stage, the assessors remain to be convinced that there are adequate human resources in the IRDA to perform effective AML/CFT supervision over this sector.

778. While the Central Government has extensive powers in terms of the appointment and dismissal of senior personnel in the regulatory authorities, and can also give directions to the authorities, there is no evidence that the government interferes with the day-to-day operations of the agencies, which appear to have broad operational independence in terms of budgetary resources and regulatory procedures. The one exception might be in respect of the state-owned banks, where the government has the direct right to appoint directors (seemingly without RBI approval), but again there is no evidence that this has been abused.

779. *Supervisory procedures:* The licensing provisions appear to be applied rigorously by the individual regulators, with due concentration given to the fitness and probity of the management. However, the scope of the regulators' legal duty to approve managerial appointments does not generally extend to non-executive directors, which is a key omission given the key role of such directors in overseeing management's performance. Instead, the regulators resort to issuing instructions to the institutions about how to carry out their own due diligence with respect to such appointments. The regulators have attested that they can remove a director if it is found, on inspection, that the director did not meet fit and proper criteria. However, the FATF standard requires that the supervisor applies fit and proper criteria prior to appointment. Moreover, the legal requirements and procedural requirements in relation to the vetting of shareholders are inconsistent with the standards. With the exception of the insurance sector, the primary legislation does not specify conditions for prior approval of significant interests in licensed institutions, although this gap has been filled, in part, by procedural arrangements introduced by the regulators by means of regulation or circular. In general, a five percent threshold has been set for prior approval to acquire shares in such institutions and this extends to direct and indirect shareholdings. Clear statutory provisions in this respect are needed.

780. All the regulators have very extensive powers of inspections and information-gathering, which they use routinely. Information is obtained through regular reporting, on-site examinations and special instructions, and the scope of the information that is routinely requested is very broad. To date, none of the regulators has been challenged on its powers to demand information from institutions, and the mood among the institutions to which the assessors spoke was that they have no defence in refusing to respond to requests. The penalties for failing to provide information or to provide false or misleading information are generally severe.

781. All the regulators routinely carry out inspections of the institutions for which they are responsible. In the case of the RBI, in particular, these are carried out at both head office and branch levels, based on a formula prescribed by the Central Office to the supervisors based in the regional offices. The regulators include AML/CFT compliance as part of the routine inspection procedure, although they all

have scope to perform targeted examinations for AML/CFT only. While this approach to inspections is perfectly reasonable, in principle, the assessors are concerned that AML/CFT risks are not being given sufficient weight in identifying which institutions (or their branches) should be inspected, and what degree of attention should be paid to the particular AML/CFT risks in the individual inspections. The AML/CFT annex to the inspection manual reads more as a checklist than a comprehensive examination manual, focusing on risk supervision.

782. The data on the sanctions applied by the regulators for AML/CFT deficiencies clearly indicate that the framework does not provide for effective, dissuasive or proportionate measures. The regulators informed the assessment team that they have taken an approach of outreach and education during the initial years of implementation of the PML Rules and related circulars, and as such have made use of administrative sanctions rather than monetary penalties. It is the authorities' view that, short of revoking an institution's licence, a monetary penalty is the final sanction that would be applied after exhausting the range of regulatory procedures (e.g. restriction on opening of new branches or expansion of business generally) that are available. That being said, the assessment team believes that if the monetary penalty is the ultimate penalty that the supervisors will apply, then the levels of monetary sanctions are definitely too low and can certainly not be considered dissuasive. For example, the average fine imposed by the RBI was the equivalent of USD 12 000 in the 43 cases where financial penalties have been levied. The average fell to USD 200 in the case of the securities sector, while no financial penalties have yet been applied in the insurance sector. These levels suggest that the sanctions are being applied for individual failures identified during transaction sampling, rather than for broader systemic failings; but even then, the sums involved would represent little more than the cost of doing business for the institutions, and would not act as a deterrent. While the fault lies in part with the regulatory approach to sanctioning (and with the legal framework that sets a very low minimum tariff), it may also be a reflection of the approach to inspections, which may have an over-reliance on formulaic compliance, and less on the overall adequacy of systems and controls. Also, given the very detailed approach currently adopted, it is surprising that neither the NABARD nor the NHB has identified deficiencies that would justify regulatory action.

783. Finally, there is one issue that is not technically in relation to compliance with the FATF standard, but which the assessors feel should be addressed in order to bring greater efficiency to the manner in which institutions handle their AML/CFT controls. At present each of the six regulatory departments of the RBI issues its own circulars specifying their requirements under the PML Rules. While these circulars are, for the most part, very similar in overall content, they are published at different times, and do contain differences of detail, for which there is not always an obvious reason. Each department examines for compliance with the specific provisions of its manual, and requires the institutions to adhere to their letter. Where institutions have more than one type of authorisation, they are required to implement in each entity the detailed procedures specified by the relevant supervisory department. In discussions with the institutions, there appeared to be a degree of legitimate concern that they were not able necessarily to implement common AML/CFT systems and controls across the spectrum of their business. While this may primarily be just a matter of efficiency, it may also give rise to operational failings in terms of group-level oversight. There would be a distinct advantage in consolidating and standardising the RBI circulars to the greatest extent possible.

3.10.2 Recommendations and Comments

- a. Commodity futures traders should be included under the PMLA.
- b. A review should be undertaken of both the levels of financial penalties for non-compliance with the AML/CFT requirements, and the procedures under which penalties are applied to ensure that they focus on systemic rather than transactional failings in institutions.
- c. The "fit and proper" tests prior to appointment should be extended to non-executive directors.

- d. The Ministry of Finance should develop and implement procedures for inspection and ongoing monitoring of India Post.
- e. A review should be undertaken of the human resourcing of the IRDA.
- f. Reviews should be undertaken by all the regulators to ensure that their procedures for targeting on-site inspections take adequate account of the AML/CFT risks of individual institutions.
- g. A review should be undertaken of the AML/CFT inspection procedures adopted by the NABARD and the NHB to ensure that they are not out of line with those adopted by the RBI itself.
- h. Consideration should be given to rationalising the circulars issued by the RBI to facilitate implementation of the overall requirements by institutions at group level.

3.10.3 Compliance with Recommendations 23, 30, 29, 17 & 25

| | Rating | Summary of factors relevant to s. 3.10 underlying overall rating |
|------|--------|--|
| R.17 | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • Sanctions applied for AML/CFT deficiencies across all sectors are not effective, proportionate or dissuasive. |
| R.23 | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • Fit and proper testing by regulators prior to appointment does not apply to Non-executive Directors. • Effectiveness issues: <ul style="list-style-type: none"> ○ Authorised Persons and Payment Service Providers, including India Post, have only recently been brought under the PMLA, and hence it is too early to assess effectiveness; ○ no inspections or ongoing monitoring by the Ministry of Finance of India Post as yet; ○ concerns that the regulators' procedures for targeting on-site inspections do not adequately take into account the AML/CFT risks of individual institutions. |
| R.30 | LC | <ul style="list-style-type: none"> • Concerns about the adequacy of staffing levels in the IRDA. • Uncertainties about the future regulatory regime for the banking activities of India Post.. |
| R.29 | LC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • Financial sanctions applied for AML/CFT deficiencies across all sectors are not effective, proportionate or dissuasive. • There is no established supervisory regime covering the banking operations of India Post. |

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and Analysis (summary)

784. As indicated in section 3.10 above, money service businesses and foreign exchange houses, which facilitate cross border money transfers, are required to be licensed or authorised by the RBI under the FEMA and the Payment and Settlement Systems Act (PSSA). They are subject to routine transaction reporting requirements and have to undergo annual inspection by the RBI for compliance with the FEMA regulations and with the circulars issued by the RBI. The scope of the AML/CFT requirements and the regulatory regime for the authorised MVT sector is described in sections 3.1-3.10 above. They are not

repeated here, although the deficiencies identified in those sections are referenced in the ratings box. One of the key issues is that the MVT sector was only brought into the AML/CFT regime in March 2009, and at the time of the on-site, there was little evidence on which to base an assessment of the effectiveness of implementation.

785. While the PSSA envisages the possibility for the RBI to authorise domestic money remitters (as distinct from those entities authorised under the FEMA to act as Indian agents for cross-border transfers), no such authorisations have yet been issued, and this activity (on a lawful basis) is currently reserved for the banks and India Post. India Post is categorised as a full fledged money changer (Authorised Person) licensed under the FEMA and falls within the definition of a financial institution since the PMLA amendment in June 2009. India Post undertakes a substantial money transfer business (in association with Western Union) and is an approved Indian Agent under the Money Transfer Service Scheme (MTSS), is therefore obligated to comply with the provisions of the MTSS Guidelines on KYC/AML/CFT that were issued to Indian Agents under MTSS, dated 27 November 2009. In addition, through the PSSA, the money transfer services are brought under the regulation and supervision of the RBI.

786. The list of Indian agents offering money transfer services, including through the normal banking activity, is placed on the RBI's website. The FEMA provides for imposition of penalty besides providing for confiscation of currency/property involved in any contravention of the provisions of the FEMA. However, contravention of provisions of the FEMA is not a criminal offence. Further, violation of provisions of the FEMA is not a predicate offence under the PMLA.

787. With regard to the intended use of such funds, the action against the recipients/transferor of such funds is taken under various acts such as (a) Unlawful Activities Prevention Act (UAPA) (as amended), if funds are meant for financing of terrorism, (b) under Foreign Contribution Regulation Act (FCRA) if funds are received as donation to certain notified bodies outside of banking channels, (c) under Prevention of Money Laundering Act (PMLA), if funds are the proceeds of crime relating to Scheduled offences and so on. In such cases the Hawala operator as well as recipient of funds is liable for criminal action as provided in the law. The Hawala transactions are being monitored by intelligence agencies exercising special investigative techniques. The 'Hawala operator' and receiver of funds for illicit activity are being booked for criminal offences depending upon the intended use of such funds. For instance, if funds are intended for financing of terrorism, then action under the UAPA by way of criminal proceedings is initiated and such funds are liable for seizure/attachment/confiscation under the UAPA and the PMLA. Similarly, if the intended purpose is for money laundering of the proceeds of foreign predicate offence, then action is initiated under the PMLA and so on. To elaborate, if the funds coming through Hawala represent the proceeds of drug trafficking in a foreign jurisdiction, the same are actionable both under PMLA and NDPSA. Further, persons concerned are liable for detention under the Conservation of Foreign Exchange and Prevention of Smuggling Activities Act (COFEPOSA), besides, other sanctions.

788. While legitimate businesses are captured under the provisions of the FEMA and the PSSA and are now also subject to the provisions of the PMLA, there exists a sizeable and demonstrated informal sector that is operating illegally. However, there seems to be some disagreement among competent authorities (and also the private sector) regarding the size and scope of the informal/Hawala/Hundi sectors, and the nature of the problem as it relates specifically to ML and FT. One view is that, as a result of the liberalisation of the foreign exchange market, there is a reduced incentive to use the Hawala system, as there is very little difference between the official and unofficial exchange rates. On the other hand, the authorities have observed that Hawala/Hundi continues to be used for low value remittances, including for terrorist financing; for smuggling, including in connection with gold and diamond trading businesses; and for facilitating invoice manipulation and compensatory payments. Apart from businesses totally outside the legal network, law enforcement authorities have detected many cases of licensed money service businesses that also conduct Hawala/Hundi transactions in the margins of their regular and recorded business conduct.

789. As indicated above, the primary enforcement authority dealing with informal remittances is the Directorate of Enforcement within the Ministry of Finance based on its specific role regarding the enforcement of the provisions of the FEMA. The division of responsibilities between the RBI and the ED is outlined in Section 3.10. The Directorate works in close co-ordination with other agencies such as State Police, Narcotics Control Bureau, Customs, Income Tax etc, which are empowered to take appropriate action under the concerned legislations of the country. The Directorate of Enforcement (ED) has identified a significant number of breaches of the FEMA provisions relating to Hawala-type transactions, as shown in the table below:

| Year | No. of cases | Amount involved (INR in million) |
|-----------------------------|--------------|-------------------------------------|
| 2006-2007 | 388 | 1103.58 |
| 2007-2008 | 160 | 1122.90 |
| 2008-2009 | 195 | 9323.22 |
| 2009-2010(up to 30.10.2009) | 154 | 899.6 |

790. The authorities have indicated that part of their frustration in trying to tackle this problem is the lack of co-operation that they receive from some countries where the transfers originate. This includes countries where Hawala activities are not licensed or regulated effectively and countries where Hawala activities are legal. To some extent, the move to suppress the activity in India has also been hampered by the foreign exchange liberalisation programme. While this has undoubtedly resulted in a reduced incentive to use Hawaladars (because of the narrowing of the exchange rate differentials), the introduction of the FEMA to replace the Foreign Exchange Regulation Act (FERA) resulted in the decriminalisation of the activity of operating without a licence. This means that only administrative fines can now be imposed for the offence (under section 3 of the FEMA) of receiving any payment or order on behalf of a person outside India, other than through an Authorised Person. The sanctions may involve fines of up to three times the amount involved in the activity, together with the confiscation of any funds that have been identified. Only in the event of default with respect to the payment of the penalty may a civil imprisonment order be served. Therefore, there is a risk that, where the activity is being undertaken primarily for criminal, rather than economic benefit, the penalties will not be considered dissuasive. However, there can be no denying the resources and expertise that the Enforcement Directorate employs in identifying and pursuing unlicensed remitters. It inherited some 15 000 cases of criminal activity under the FERA, and had managed to clear about 12 000 cases by end-2009, but this remains the primary focus of its work on Hawala. A much more limited number of cases have been referred to it under the FEMA. Eleven persons have been found to be repeat offenders under FEMA to date.

3.11.2 Recommendations and Comments

791. India should take action to address the deficiencies identified in relation to the implementation of the FATF Recommendations, as identified in sections 3.1 to 3.10 of this report, in relation to MVTS providers.

3.11.3 Compliance with Special Recommendation VI

| | Rating | Summary of factors relative to s.3.11 underlying overall rating |
|-------|--------|---|
| SR.VI | LC | <ul style="list-style-type: none"> The application of the FATF Recommendations to MVTS providers suffers from the same deficiencies as identified in relation to the rest of the financial sector (see sections 3.1 to 3.10 of this report). |

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Scope issue

792. DNFBPs conducting business in India include casinos, lawyers, real estate agents, accountants, company secretaries, gold dealers, and dealers in precious metals and stones. There is no free-standing profession of trust and company service providers, but these services are provided by the other professionals, especially accountants and company secretaries. The nature of the activities of each sector (insofar as they are relevant to the FATF standards) is described in Section 1 of this report. With the exception of casinos⁷² (which only operate in the State of Goa, and which were brought under the PMLA with effect from 1 June 2009), these businesses are not subject to the PMLA provisions. However, some guidelines that have relevance to AML/CFT have been drawn up by the industry and professional bodies. These are described briefly in this section of the report, but have no impact on the overall assessment of compliance with the FATF standards.

793. As part of the process towards deciding when and if to include the remaining DNFBP sectors within the provisions of the PMLA, the authorities have undertaken a formal risk assessment. An inter-ministerial committee (consisting of members from concerned ministries, law enforcement agencies and FIU-IND) was constituted to consider the following aspects:

- money laundering/terrorist financing methods used in the various sectors;
- assessment of the effectiveness of existing controls; and
- suggested controls/mechanisms to address the identified gaps.

794. The conclusions from this exercise about the risk posed by each sector have been summarised in the following chart.

| | | | | |
|---------------|------------|---------|----------------------------|-------------|
| Vulnerability | High (3) | | | |
| | Medium (2) | Casinos | Precious metals and stones | Real estate |
| | Low (1) | Lawyers | Accountants | |
| | | Low (1) | Medium (2) | High (3) |
| | Threat | | | |

⁷² Comprising both ship-based and land-based facilities. Internet casinos do not exist in India.

795. As a result of this assessment, the committee proposed a number of measures to address the perceived risks in respect of each of the sectors, but none involved bringing them within the PMLA, since this was considered to be outside the scope of the committee's terms of reference. Instead the committee looked at building on the existing governance structures that apply to the sectors.

796. In conjunction with this, consultants were appointed to conduct a further study of the DNFBP sectors with the following terms of reference. The scope of the study covered the following aspects:

- a. Understanding of key characteristics of the DNFBPs:
 - Assess the size (in terms of revenue generation and number of players) and composition of the DNFBPs
 - Identify the size and nature of activities
 - Categorize types of products and services offered
 - Profile the types of customers serviced
- b. Analysis of transactions in the DNFBPs:
 - Identify the ownership structure of the businesses
 - Identify the chain of activities through which financial transactions take place to buy a product or service
 - Evaluate the nature of payment systems when offering the services/products, and the prevalence of cash-based transactions
- c. Assessment of the current regulatory mechanism in the DNFBPs (if any):
 - Assess the corporate governance arrangements (if any)
 - Study the existing licensing, supervisory and regulatory regime and its coverage
 - Existing requirements for customer identification, reporting and record-keeping.

797. According to the Indian authorities, the decision on whether to include the designated businesses (precious gems, stones, real estate) under the PMLA will be based on such issues as market share of the informal sector in each activity; the availability of information on the entities making up the sector; and the presence and scope of any existing licensing, supervisory or regulatory regime. Furthermore, the possible inclusion of the designated professions (lawyers, accountants, etc.) will depend on resolving issues relating to the STR obligation and professional privilege. In discussions with the company secretaries and accountancy sectors, the assessment team was advised that neither profession had any disagreement with being subject to the PMLA, but that there were ongoing discussions between the accountants and the government over the potential impact on client confidentiality. In addition, since January 2008, the FIU-IND has initiated an outreach programme to the various professional bodies, such as the Bar Council of India, the Institute of Chartered Accountants of India (ICAI) and the Institute of Company Secretaries of India (ICSI) to sensitise them to the importance of AML/CFT issues.

4.1 Customer due diligence and record-keeping (R.12) (applying R.5, 6, and 8 to 11)

4.1.1 Description and Analysis

798. With the introduction of the amendments to the PMLA in June 2009, casinos were included within the definition of financial institutions. As a result, all the provisions of the PMLA and the accompanying Rules became applicable to this sector. However, casinos do not constitute financial

institutions in the context of the RBI circulars, which, therefore, have no relevance to the casino sector. At the time of the on-site visit, the Home Department of the Government of Goa had drafted a set of guidelines to be issued under the PML Rules. These guidelines, which were subsequently issued on 24 December 2009 (and which constitute “other enforceable means” on the same basis as those issued by the financial regulators), simply reiterate the basic requirements of the PML Rules, and add nothing beyond what the PMLA and the Rules themselves require. Therefore, the obligations on the casino sector are identical (and limited) to those listed under the heading “All institutions covered by the PMLA” in section 3.2 above. In summary, these require casino operators to:

- a. verify and maintain a record of the identity and current address of the customer when opening an account or when undertaking an occasional transaction of INR 50 000 (USD 1 000) or more;
- b. verify the identity using a range of documents specified for individuals, corporate entities or legal arrangements;
- c. identify the beneficial owner and take reasonable measures to verify his/her identity;
- d. exercise ongoing due diligence; and
- e. maintain records for ten years in line with the requirements of section 12 of the PMLA and the accompanying Rules (as described in Section 3.5. above).

799. The PMLA does not apply to the other DNFBP sectors. There are, however, some incidental procedures, guidelines or codes of conduct that assist with customer identification, although these have no statutory underpinning for AML/CFT purposes.

- a. In the **real estate sector**, when the transfer of title to a property takes place, the registrar is required to obtain the identity documents of both the buyer and the seller, and to take fingerprints and photographs. Any transaction above INR 3 million (USD 60 000) must be reported to the tax authorities.
- b. Following the 2004 APG evaluation visit, the **Gem and Jewellery Export Promotion Council** commissioned an AML/CFT handbook for its members, drawn from the procedures adopted by a leading money exchange company. This addresses a range of issues relating to CDD, record-keeping, systems and controls and training. Compliance with the guidelines is stated to be a requirement for membership of the Council, but there are no effective disciplinary powers through which to enforce compliance.
- c. The Code of Ethics of the **Institute of Chartered Accountants of India** imposes an obligation to undertake a form of CDD as part of the client acceptance procedures. Section 210.4 of the Code specifies that “appropriate safeguards may include obtaining knowledge and understanding of the client, its owners, managers and those responsible for its governance and business activities”. The Code is enforceable under the Institute’s disciplinary procedures.
- d. Although the Council of the **Institute of Company Secretaries of India** has disciplinary powers over its members, it has not issued any guidelines or codes which address AML/CFT-related matters. However, at the time of the on-site visit, the Institute was giving consideration to producing some form of guidance for its members.

Implementation and effectiveness

800. At the time of the on-site visit, the casino sector had been subject to the PMLA for less than six months. Therefore, there was no real basis for assessing the effectiveness of implementation. By most

benchmarks, the sector currently appears to pose a relatively low risk for money laundering, based on the following features:

- a. The majority of the licensed casinos (*i.e.* those based in the hotels) provide only slot machines and electronic games which are subject to low limits;
- b. Fewer than 5% of the customers (almost exclusively on the ship-based operations) undertake transactions of USD 1 000 or more;
- c. Although account-based relationships are permitted in principle, none of the casinos currently offer such a facility, and have no plans to do so; and
- d. All payouts are in cash (rather than cheque or any other instrument) and, under the FEMA provisions, must be paid in rupees, irrespective of the currency brought in by the customer.

801. That said, the current very basic provisions applicable to the sector are posing some challenges. The operators concede that they face difficulties in monitoring customers who might undertake multiple transactions which, when aggregated, breach the INR 50 000 threshold for identification. This is caused, in part, by the preference to have customers purchase chips at the tables (rather than at the cage, where all cashing-out takes place) so that the profitability of each table is more easily assessed. Moreover, the assessors were advised that the practice is to seek identification at the entrance to the casino only, and so it is not clear how the link would be established between the transactions and the identified customer. In the first six months following the implementation of the amendments to the PMLA, the Home Department of the Government of Goa, which has responsibility for regulating the sector, had visited all the casinos twice, in order to advise them on the necessary measures to implement the law. It is important that this process should continue to bring the operators up to an appropriate level of compliance while the business remains relatively low risk.

4.1.2 Recommendations and Comments

802. It is clearly very early days in the extension of the AML/CFT obligations to the DNFBP sectors. While the PMLA and the accompanying rules have been applied to the casino sector, there have been no substantive additional provisions imposed by the regulators in Goa. Therefore, it is essential that the Home Department of the Government of Goa should undertake a thorough study of the FATF standards and determine what additional instruction needs to be applied to the casinos in order to address the perceived risks and to comply with the standards. In this respect, it will clearly be helpful to review the circulars issued by the financial sector regulators and draw from their experience.

803. As regards the other DNFBP sectors, it is important that the Government extend the PMLA to the businesses and professions as soon as possible. While the FATF standard does not envisage the complete exclusion (on a risk basis) of any of the DNFBPs from meeting the AML/CFT obligations, since they are all perceived to present a material risk, it is clearly appropriate to consider, on a risk-sensitive basis, the extent to which the range of requirements need to be applied.

4.1.3 Compliance with Recommendation 12

| | Rating | Summary of factors relative to s.4.1 underlying overall rating |
|------|--------|--|
| R.12 | NC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to any of the DNFBP sectors, with the exception of casinos. • Only the basic requirements of the PMLA and the accompanying rules apply to casinos, and these do not address much of the detail required under the FATF standards. • Effectiveness issue: <ul style="list-style-type: none"> ○ extension of the PMLA to the casino sector is very recent and there is insufficient evidence of effective implementation. |

4.2 Suspicious transaction reporting (R.16) (applying R.13 to 15 & 21)

4.2.1 Description and Analysis

Applying R.13 and SR.IV (STR Reporting)

804. Only casinos are obligated to file STRs under the PMLA, on the same basis as for financial institutions, *i.e.* a transaction which:

- a. gives rise to reasonable grounds to suspect that it may involve proceeds of a predicate offence;
- b. appears to be made in circumstances of unusual or unjustified complexity;
- c. appears to have no economic rational or bona fide purpose; and
- d. gives rise to reasonable grounds to suspect that it may involve terrorist financing.

805. At the time of the on-site visit, no such reports had been filed by any of the operators within the first six months of their being subject to the PMLA.

Applying R.14 (Tipping-off)

806. Casino operators and their officers are provided with statutory protection under section 14 of the PMLA in respect of any reports filed with the FIU, but only against civil proceedings. The 12 November 2009 amendment to the PMLA rules provides that a casino (as a financial institution) “shall keep the fact of furnishing information in respect of [STRs] strictly confidential. This appears to extend the tipping-off prohibition broadly to cover all stages of the reporting process.

Applying R.15 and R.22 (Internal controls)

807. The PMLA and its accompanying Rules provide very little direction with respect to the internal procedures, policies and controls that are expected of casino operators. These relate only to the implementation of a client identification programme, certain record-keeping requirements, the procedures for supplying information to the FIU, and the appointment of a designated person to act as the money laundering reporting officer, described as the “Principal Officer”. The defined role of the Principal Officer is far narrower than that of a money-laundering compliance officer and relates only to the transmission of reports to the FIU. The development of internal procedures to detect and report STRs is loosely phrased: “institutions may evolve an internal mechanism for furnishing such information in such form and at such intervals as may be directed by the regulatory authorities” (Rule 7(3) of the Rules). The Rules are silent on the need for a co-ordinated AML/CFT programme, independent audit procedures, and structured staff training. The guidelines developed by the Home Department of the Government of Goa largely repeat the provisions of the PMLA and the Rules, and add nothing by way of additional requirements.

4.2.2 Recommendations and Comments

808. As with the issues addressed under Recommendation 12, the authorities in Goa should review the need to issue further enforceable guidance to the casino sector, especially in relation to the implementation of appropriate internal systems and controls. This is especially important in the context of the offshore casinos, which pose the greater (albeit still quite low) risk.

809. More generally, appropriate obligations will need to be introduced for the other DNFBP sectors once they are brought under the PMLA.

4.2.3 Compliance with Recommendation 16

| | Rating | Summary of factors relative to s.4.2 underlying overall rating |
|------|--------|---|
| R.16 | NC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to any of the DNFBP sectors, with the exception of casinos. • Only the basic requirements of the PMLA and the accompanying rules apply to casinos, and these do not address much of the detail required under the FATF standards. • Implementation issue: <ul style="list-style-type: none"> ○ extension of the PMLA to the casino sector is very recent and there is insufficient evidence of effective implementation. |

4.3 Regulation, supervision and monitoring (R.24-25)

4.3.1 Description and Analysis

810. Casino operators are licensed and supervised by a small unit within the Home Department of the Government of Goa. The governing legislation is the Goa, Daman and Diu Public Gambling Act of 1976 (as amended), and its accompanying regulations. These provide the authorities with powers of authorisation, inspection and sanction. Onshore casinos may only be established in five-star hotels, and are restricted to electronic amusement and slot machines (*i.e.* no live games are permitted). Licenses are subject to renewal every five years, unless previously revoked. Offshore casinos are permitted to operate live games, subject to the vessel being licensed by the appropriate Goan shipping authorities, and having a non-objection certificate from the Captain of Ports. Unlike many other ship-based casino operations elsewhere in the world, those licensed in Goa must remain within Indian territorial waters, and they are effectively limited to the river estuary. The licensing provisions focus primarily on the submission of certain specified documentation, but they also require that the authorities make “such enquiry as may be necessary”. The regulators advised the assessment team that these enquiries would involve “fit and proper” checks on the operators only, and not on the proposed management.

811. Section 8 of the Notification of 9 November 1995 (issued under the Goa, Daman and Diu Public Gambling Act) gives the regulator the power to enter any premises at any reasonable time to inspect compliance with the provisions of the Act, and it also requires the licensee to provide every reasonable assistance to the regulator in such circumstances. The regulator also has the power to seek records and other documents as and when necessary. Section 8(iii) makes it an offence for anyone to prevent or obstruct the entry of the regulator (or any person appointed by it), but the penalty is only INR 500 (USD 10), which would fail to act as a meaningful deterrent. Moreover, the sanction for the regulator’s powers under these provisions appear, under section 8(i) of the Notification, to be limited to enforcement of the provisions of the Goa, Daman and Diu Public Gambling Act alone, and it is not clear how these provisions could be used to enforce the provisions of the PMLA and the Rules.

812. Under section 6 of the Notification, revocation of the license may take place in the event of the breach of any of the terms and conditions of the licence, subject to the operator being given notice of the intention and an opportunity to be heard. Appeal against a decision of the regulator is to the Appellate Authority. To date, eleven onshore and six offshore licences have been granted (although only three offshore licensees have started business). The legislation does not contain any other sanctioning provisions, except revocation of the licence. No sanctions have yet been applied.

813. Section 12 of the PMLA imposes obligations on all covered institutions for maintaining records of transactions, furnishing information of transactions and maintenance of records, and section 13 empowers the Director of the FIU-IND to impose a fine of not less than INR 10 000 (USD 200), but which may extend to INR 100 000 (USD 2 000), for each failure by covered institutions to comply with the

provisions of Section 12. There are no sanctioning provisions within the PML Rules, since it was clearly envisaged that these would be implemented under cover of the broader powers given to the financial sector regulators under their respective statutes. In the absence of any such similar powers for the casino regulator, it is unclear what the legal authority of the regulator would be to apply sanctions for breaches of its AML/CFT circular, apart from revocation of the licence, which is the only course available under the casino legislation. The very recent extension of the PMLA to the casino sector means that there has been no opportunity to test either the level of compliance with the obligations under the Act, or the application of appropriate sanctions.

814. None of the other DNFBP sectors is subject to supervision by a competent authority for AML/CFT purposes. Some degree of oversight of the professional activities of the other sectors does, however, take place, and may provide some basis for future regulation when the relevant businesses and professions are brought within the PMLA:

- a. Registration of real estate agents is required in only a minority of States, and consequently the authorities have no knowledge of the number of such businesses in existence. The Central Government is preparing a model law, which it hopes that the States will adopt, but this would only impose a duty on the developers and promoters to oversee the activities of agents in the interests of the consumer.
- b. The Gem and Jewellery Export Promotion Council was established by the Ministry of Commerce and Industry in 1966. Its primary function is to promote the export of gems and jewellery from India, but it also has a role in providing guidance and training to its members (of which there are 5 500), as well as advising government on matters relating to the industry. In December 2006, the Council issued AML guidelines to its members, largely on the basis that this would promote their standing in the key export market of the US. The guidelines are described as mandatory for the membership, but the Council is not a self-regulatory organisation, and has no enforcement powers other than to terminate membership. Membership of the Council is not a necessary condition to engage in the gem and jewellery business.
- c. The Institute of Chartered Accountants of India was established by Act of Parliament in 1949. It has about 159 000 members, of whom 72 000 are in private practice. It is a criminal offence to hold oneself out as a chartered accountant without being a member of the ICAI. The Institute's Council has the statutory authority to define the activities in which its members may engage. These currently include the provision of management consultancy services, which incorporates a broad range of financial management services and investment counselling. The ICAI is empowered to formulate ethical standards which are mandatory for all members, and can enforce these through its statutory disciplinary powers. The current Code of Ethics does not contain any AML/CFT measures, although the client acceptance procedures contain some basic elements of a CDD process. However, the Institute has published a number of studies on ML risk for the accountancy profession, and has included the topic, on an *ad hoc* basis, in its professional training.
- d. Responsibility for professional standards within the legal profession is vested primarily in the nineteen State Bar Councils. The Bar Council of India acts as the appellate body for decisions made by the state authorities.
- e. The Institute of Company Secretaries of India was established under the Company Secretaries Act of 1980, and has a membership of about 24 000, of whom 3 430 are in independent private practice. The range of services that may be provided is defined in the Act (and includes company formation and management), although the Institute's Council has broad discretion to expand these. However, there is no clear provision within the Act prohibiting someone from acting as a company secretary without being a member of the Institute. The

Institute has statutory responsibility for overseeing compliance with the code of conduct provided for under the Act, and also has the power to issue mandatory guidelines to its members. Compliance is enforced through a Disciplinary Board and Committee, with final recourse to an Appellate Authority. However, none of the guidelines addresses issues directly relevant to AML/CFT measures (including client acceptance procedures), although various outreach initiatives have taken place, and AML/CFT has been included in the professional training programme.

Recommendation 25 (Guidance for DNFBP other than guidance on STRs)

815. The Government of Goa has produced guidelines for the casino industry, although these do little more than reference the provisions of the PMLA and the accompanying Rules. Unlike the equivalent circulars issued by the financial sector regulators, they do not specify additional requirements or provide substantive guidance to the casino operators on how to fulfil their statutory obligations. However, the FIU-IND has undertaken several outreach programmes to both the casino operators and the Government of Goa to explain the general obligations under the PMLA, and to provide guidance on the types of suspicious transactions in the casino sector.

816. While the authorities (especially the FIU-IND) have been engaging with the other DNFBP sectors (not least in the context of its risk assessment project), no formal guidance has been offered since none of the other sectors is covered by the PMLA. As indicated above, certain industry bodies have produced guidelines for their members, but these are not enforceable within the context of the AML/CFT regime in India.

4.3.2 Recommendations and Comments

817. It is recommended that the regulatory framework for the casino sector be extended in order to:

- give the authorities statutory powers to apply “fit and proper” tests to the owners, operators and managers of casinos;
- give the regulator the statutory authority to use its powers of inspection, etc., in order to enforce compliance with the provisions of the PMLA;
- increase the penalty for obstructing access by the regulator, in order to make it effective and dissuasive;
- make specific provision for sanctions to be applied for breaches of the PMLA, the accompanying Rules and any relevant instructions that the regulator may issue from time to time; and
- broaden the scope of the sanctions that may be applied, so that there is a range of options that might be applied effectively.

818. The scope of the written guidance provided to the casino sector to assist with the implementation of the PML Rules needs to be extended.

4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

| | Rating | Summary of factors relative to s.4.3 underlying overall rating |
|------|--------|--|
| R.24 | NC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to any of the DNFBP sectors, with the exception of casinos. • With respect to the casino sector: <ul style="list-style-type: none"> ○ No statutory “fit and proper” tests for owners, operators and managers. ○ Insufficient range of sanctions available to the regulator to permit a proportionate response to identified deficiencies. ○ Doubts about the statutory authority of the regulator to enforce compliance with the PML Rules and its own AML/CFT circular. ○ Lack of dissuasive sanctions for obstructing the regulator’s right to inspect. |
| R.25 | LC | <ul style="list-style-type: none"> • Written guidance provided to the casino sector to assist with the implementation of the PML rules is limited in scope. |

4.4 Other non-financial businesses and professions

Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

Application of FATF Recommendations to other non-financial businesses and professions

819. Section 2(ja) of the PMLA provides for the Central Government to prescribe such activities as it thinks appropriate as a “designated business or profession” for the purposes of the Act. Apart from the casino sector, no non-financial activities have been brought under the PMLA, and no consideration has been given to doing so.

Measures to encourage modern secure techniques for conducting financial transactions

820. India has taken various measures to encourage the development and use of modern and secure techniques for conducting financial transactions. In the Indian securities market, all transactions are settled through payment and settlement system wherein cash transactions are not permitted. The main stock exchanges (*i.e.* the NSE and BSE) are fully automated exchanges with a system of electronics trading wherein each transaction can be monitored and recorded. The SEBI has implemented an Integrated Market Surveillance System (IMSS) across stock exchanges and across market segments (cash and derivatives markets).

821. In the banking sector, the Electronic Funds Transfer System (EFT) was started in 1994 which is a retail funds transfer system enabling customers to transfer funds from one region to another, without any physical movement of instruments. The Real Time Gross Settlement System (RTGS) was started in 2004 to bring safety and efficiency in large value payments. The entire inter-bank clearing system shifted to this secure payment system platform. The retail clearing system in Mumbai (both paper based and electronic) as well as interbank government securities, foreign exchange and the money market clearing system operated by the central counterpart, the Clearing Corporation of India, are settled through the RTGS system. The National Electronics Funds Transfer System (NEFT) came into operation in 2005. This system facilitates electronic retail transfer between bank branches using Structured Financial Messaging Solution (SFMS) and secured by Public Key Infrastructure (PKI) technology. Eventually EFT will be subsumed in the NEFT system. The electronic clearing service (ECS) was set up to facilitate payments from one source to many recipients (ECS Credit) (*e.g.* for payment of salary, dividend, interest, etc.) and vice-versa (ECS debit) (*e.g.* for utility bill payment, insurance premiums, loan repayments, etc.). During October 2008 a

centralised version of ECS Credit, known as National-ECS (NECS), was launched. NECS leverages on the centralised counting system in banks, and the account of a bank that is submitting/receiving payment instructions is debited/credited centrally at Mumbai. The branches participating in NECS can be located anywhere across the country. Eventually all electronic retail payments will be routed through either the NEFT or NECS system.

822. At a retail level, the usage of Credit and Debit Cards has picked up, and nearly 2 million cards are added each month and the card base exceeds 100 million. To encourage non-cash transactions, licensing policy for off-site and on-site Automated Teller Machines (ATMs) has been liberalised.

823. In the insurance sector, IRDA has issued instructions requiring insurance companies not to accept cash towards insurance premium/proposal deposits above INR 50 000.

4.4.2 Recommendations and Comments

824. India should consider extending the AML/CFT provisions to non-financial businesses and professions (other than DNFBPs).

4.4.3 Compliance with Recommendation 20

| | Rating | Summary of factors relative to s.4.4 underlying overall rating |
|------|--------|--|
| R.20 | LC | <ul style="list-style-type: none"> No consideration given to extending the AML/CFT provisions to other than DNFBPs. |

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

Recommendation 33

825. A variety of forms of legal persons/entities exist in India governed by different statutes and laws as follows:

| Legal Persons | Governing laws | Number of entities (as at December 2009) |
|---|---|---|
| Public Limited Companies | Companies Act, 1956 | 82 058 |
| Private Limited Companies | Companies Act, 1956 | 704 716 |
| Partnership | Indian Partnership Act, 1932 | unknown |
| Limited Liability Partnership | Limited Liabilities Partnership Act, 2008 | 440 |
| Sole Proprietorships | Governed by State legislation | unknown |
| Hindu Undivided Family (HUF) Businesses | Customary Hindu law; not formalised | unknown |

826. Private limited companies may have from two to 50 members (shareholders); public companies must have a minimum of seven members with no limit on the maximum number. Shares of public companies may be either unlisted or listed. In the latter they may be traded on one or more stock exchanges. Of the number of incorporated companies, both public and private, 2 609 are foreign companies. Limited Liability Partnerships (LLPs) are incorporated entities under the Limited Liabilities Partnership Act, 2008, which came into force on 31 March 2009.

5.1.1 Description and Analysis

Central Registration System

Companies

827. The Registrar of Companies (ROC) is the central registering authority for companies in India and it is a mandatory obligation for companies to register. There are 20 registries in India and companies can register with any of them, but incorporation at any of these registries does not prohibit doing business in another location in India. Before a certificate of incorporation can be issued the following documents must be filed with the ROC:

- a. the Memorandum of Association which states the objectives and purposes for which the company has been formed; and
- b. the Articles of Association which outlines the rules and regulations for achieving those objectives and purposes.

828. Subscribers to these instruments must sign them both and provide their name, address, description and occupation (Companies Act ss.15 and 30) in addition to the name of the company. Subscribers are deemed directors until other directors are appointed. Additional director information of a personal nature is collected under sections 266A to 266G of the Companies (Amendment) Act, 1956. Under those sections a “Director Identification Number” (DIN) must be obtained by proof of identity, including a photograph and proof of residence both which must be attested.

829. A company must have a registered office in India and section 150 of the Companies Act requires every company to keep a register of members (shareholders) at that office containing:

- a. the name, address and occupation of each member;
- b. the shares held and paid by each member; and
- c. the date each person was entered as, or ceased to be, a member.

A foreign company registered in India is required to have a registered office in India but is not required to maintain a shareholders’ (or members’) register or other records.

830. It is an offence not to keep this information specified in the previous paragraph. A fine of up to INR 500 (approximately USD 10) can be imposed for each day during which the default continues. It should be noted, however, that the scope of shareholder information is limited.

831. While section 187C of the Companies Act and the Companies (Declaration of Beneficial Interest in Shares) Rules, 1975 require that a registered shareholder must declare to the ROC who the beneficial owner of a share or shares (other than the registered owner) is within 30 days of issuance of the certificate (and any changes thereafter), the Rules do not extend beyond the immediate beneficial owner. Moreover, the term “beneficial owner” is not defined in the Companies Act or in the relevant Rules and so it is not clear what is intended within the scope of this term. As noted below, a Hindu Undivided Family (HUF) may hold shares in a company but only the “Karta” (see below for meaning) of a HUF (as the shareholder on behalf of the other HUF members) is required to be disclosed in the shareholder register.

832. There is no prohibition in the Companies Act on directors appointing nominees to act in their place and, in fact, Schedule II to this Act contemplates that they can. The Companies Act does not, however, contain any provision for the disclosure of undisclosed principal directors represented by a nominee in a company’s corporate records. It is possible therefore for a nominee director, including a

company, to act on behalf, and at the direction, of an undisclosed principal in the operations of a company, even though the nominee director has a DIN. Likewise, there is no prohibition in the Companies Act against nominee shareholders. And, in fact, the Trustees (Declaration of Holdings of Shares and Debentures) Rules, 1964 provides that shares in a company held in a trust are subject to information disclosure about the beneficial owner. The required disclosure, however, is limited to information about the trust and the beneficiaries of the trust and does not extend beyond the immediate beneficial owner and therefore does not include collecting information on the shareholders of a beneficial owner which is a legal person.

833. Every company is required to file an Annual Return with the ROC (Companies Act s.159 and Schedule 5) containing information on shareholders and debenture holders, past and present, and its directors, managing directors, managers and secretaries, past and present. With respect to shareholders named in the Annual Return, there is no requirement to inform the ROC of changes in shareholders during any particular year – only the names and shareholdings need to be disclosed at the time of filing of the return. Other than the information in a DIN, more comprehensive background information on directors is not collected during registration, incorporation and annual reporting and at the time of the on-site visit, there was no legal requirement to check directors' names against international terrorist lists (UNSCR 1267) or domestic terrorist lists (UNSCR 1373).

834. Company Secretaries provide a variety of services to companies, including acting as formation agents (Company Secretaries Act s.2(2)(b)). There is nothing in that Act, however, requiring company secretaries to collect and hold identifying information on shareholders or directors of companies they form or act for in one or other capacity, including nominee directors or holders of beneficial interests in shares.

Partnerships – General and Limited Liability

835. There are two forms of partnerships in India: general partnerships and limited liability partnerships (LLPs).

836. General partnerships may register under the Partnership Act, 1932 (there is no strict requirement to register) and if they do so, the names and addresses of the partners, together with joining dates, must be provided to the State Registrar of Firms within one year of registration (s.58). There is no prohibition on companies from being partners in a partnership.

837. A limited liability partnership is a separate legal entity (Limited Liability Partnership Act, 2008 s.3) which combines features of a partnership and a company, including perpetual succession. A LLP enables the partners (a minimum of two) to limit their liability in this regard in the same manner as shareholders in a company. A company may be a partner in a LLP (s.5). The reduction of risk through LLPs encourages business vehicles like firms of professionals (lawyers, accountants, etc.) to grow in size. A LLP is advantageous because of the following characteristics: comparatively lower compliance requirements, easy to manage and run, and also easy to wind-up and dissolve. Partners are not liable for the acts of the other partners and importantly, no minimum alternate tax applies. LLPs must be registered with, and incorporated through, the ROC. The information filed must include the address of the registered office and the names and addresses of all partners (s.11(2)). All designated partners of an LLP are required to obtain a “Designated Partner Identification Number” (DPIN) which is obtained by proof of identity, including a photograph and proof of residence both which must be attested.

Sole Proprietorships

838. Sole proprietors are not separate legal entities but simply persons who undertake business under a business name with no requirement to register. The proprietor is solely responsible for all acts and liabilities of his or her business.

Hindu Undivided Family Businesses

839. Hindu undivided families (HUF) are part of traditional Hindu customary law and are legal entities comprised of members of a nuclear or extended family. HUFs are unique under Indian law and have some elements in common with a trust or partnership, but in other respects they are different. For instance, a HUF is defined as a “person” (unlike a trust) under section 2 of the PMLA. A HUF can hold assets such as company shares, securities, jewellery, and moveable and immoveable property.

840. Property, whether moveable or immoveable, held in an HUF, is held in the name of the “Karta” (usually the senior family member) but there is no legal requirement on the Karta or other HUF members to maintain records with the names of beneficial owners of assets within these legal entities. No separate instrument or document is required to be executed for the creation or continuance of a HUF. But if a HUF purports to create or extinguish rights in land, it must be memorialised in writing and registered under the Registration Act, 1908. However, where an arrangement does not create or extinguish any right in immoveable properties, and a written document is executed, it does not fall within the ambit of section 17(1)(b) of the Registration Act and so it does not require registration⁷³.

841. HUFs can operate as businesses and can be composed of a large number of branches/families - each branch itself being a HUF and so also the sub-branches of more branches. Members of a HUF can live separately and such an act would not automatically amount to partition of the HUF.

842. There are tax advantages granted to HUFs but tax returns are filed in the name of the Karta only. A Permanent Account Number (PAN) card may be issued by the Income Tax Department in the name of a HUF and an account established for filing tax returns. Some Indian financial institutions may seek identification information from a HUF before opening business accounts for HUF businesses, but Indian officials advised that this was a matter of practice and not followed by all financial institutions. Financial institutions spoken to by the evaluation team indicated that identification information is only sought about the Karta and not the other HUF members.

843. The number of HUF's, including HUF businesses, throughout India is unknown. Indian officials advised that these entities are declining in use as the traditional family unit declines but a large number still continue to operate.

Access to information by competent authorities

844. Regulatory, supervisory and law enforcement authorities (including Police, Income Tax authorities, FIU and securities regulators) have a variety of powers that enable them to secure information about the control and ownership of legal persons in India both from publicly available sources and through a variety of coercive measures.

845. Coercive measures include production orders, search warrants in justifiable circumstances and court ordered inspections in other circumstances. Since foreign companies are not required to keep a copy of their shareholder register in India, access to the shareholder register of foreign companies is available only through a formal mutual legal assistance process. This means that such information is not available to the Indian authorities on a timely basis. Law enforcement authorities may also take statements from witnesses. For publicly available information, those authorities may search the appropriate corporate registries in addition to other publicly available databases relating to companies for any relevant information.

⁷³ *Roshan Singh Vs. Zile Singh* - AIR 1988 SC 881.

Bearer shares/Bearer share warrants

846. Bearer shares are not permitted in India by virtue of section 84 of Companies Act and Rule 5 of the Companies (Issue of Share Certificates) Rules, 1960 both of which require that every certificate has to specify the name(s) of the person(s) in whose favour the certificate is issued, the shares to which it relates and the amount paid up. However, the Companies Act does permit the issuance of “share warrants to bearer” (or bearer share warrants) by public companies where (1) their articles of incorporation permit them to be issued; and (2) the Central Government permits their issuance (s.114). A bearer share warrant entitles the bearer thereof to redeem the warrant for the issued shares.

847. Indian authorities indicated that no public company has yet requested Central Government approval to issue such warrants. Indian authorities also indicated that if a public company were to request approval to issue bearer share warrants that the Central Government would look at a number of points including, whether the shares are fully paid up and no unpaid call is pending on shares; whether a Members’ Resolution has authorised share warrants to issue; the number of shares proposed to be issued against one such share warrant; the terms and conditions of the share warrants; the financial position/profitability of the company for the last three years is satisfactory; the details of persons to whom share warrants are proposed to be issued first time; and the details/percentage of proposed dividend to be paid. These criteria are not specified in any instrument but have been promulgated by the Ministry of Corporate Affairs on a purely *ad hoc* basis only.

Implementation and effectiveness

848. India’s corporate registry and information collection system does not focus on obtaining information relating to the beneficial owner or controller of companies or limited liability partnerships. The information maintained (including changes in information) relates almost solely to persons and other corporations that are the immediate owners or controllers of a company. In addition, there is the possibility that nominee directors act on behalf, and at the direction, of an undisclosed principal in the operations of a company.

849. HUFs are unique in India and also present challenges for identification of beneficial ownership of common assets. For those HUFs that carry on business in India there should be safeguards in place, including measures to ensure that beneficial ownership information is collected and maintained, to ensure that they cannot be exploited for money laundering and terrorist financing. At the moment (notwithstanding that the use of these traditional family entities is declining in India), no safeguards exist.

850. The registry is not required to cross-reference applications for company formations against the UN 1267 and 1373 terrorist lists issued by other agencies. Legal requirements such as these could act to mitigate to some extent the threat that arises through the use of legal persons to perpetrate terrorist financing.

851. The Companies Act permits ownership of public companies through bearer share warrants but there appear to be adequate safeguards in place to ensure that beneficial owners of these instruments are identified.

5.1.2 Recommendations and Comments

852. India should ensure that information on beneficial ownership of legal persons is collected by either the corporate registry, within corporate records held by legal persons, or by company secretaries. India should also prohibit nominee directors and nominee shareholders, or (alternatively) establish measures to mitigate the risk of ML and FT associated with those kinds of directors and shareholders.

853. There should be measures in place to ensure that beneficial ownership information relating to Hindu Undivided Family (HUF) businesses is available through a requirement for HUFs to register with a central registry and maintain beneficial ownership information or through other measures such as a requirement for all HUFs to obtain PANs and to maintain information on all beneficial ownership information available to law enforcement or other authorities on request.

854. India should take measures to ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis. The current powers of the competent authorities are hampered to the extent that the repositories of information from which the authorities could obtain information do not maintain sufficient beneficial ownership information.

855. India should also formalise the set of criteria established by the Ministry of Corporate Affairs applied to the issuance of bearer share warrants in a guideline, rule or other instrument rather than in unpublished *ad hoc* format.

5.1.3 Compliance with Recommendations 33

| | Rating | Summary of factors relative to s.5.1 underlying overall rating |
|------|--------|--|
| R.33 | PC | <ul style="list-style-type: none"> Information on additional beneficial ownership of legal persons beyond the immediate beneficial owner is not required to be collected by either the corporate registry, within corporate records held by legal persons, or by company secretaries. There are no measures in place to prevent the unlawful use of HUFs in relation to ML or FT – for instance, HUFs are not required to maintain information on beneficial ownership. While law enforcement and other authorities have sufficient powers to access current and accurate information on beneficial ownership of legal persons (in particular foreign companies), this is not possible in a timely fashion. |

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

Recommendation 34

Categories of trusts in India

856. There are three general categories of trusts in India:

- private trusts: to benefit selected persons;
- charitable or public trusts (including religious trusts): to benefit the public at large.
- wakfs: for performing certain Islamic religious activities.

Private trusts

857. The Indian Trusts Act, 1882 defines and governs the law relating to private trusts and their trustees. The Act does not apply to charitable/public trusts or to religious trusts (wakfs). Under India's common law system, a variety of forms of private trusts, including express trusts, are recognised. The constituent elements of Indian trusts are the same as in other common law jurisdictions (settlor, trustee and identified beneficiary), one or all of whom may be natural or legal persons. The same person may act in all three capacities in relation to a particular trust. However, there is no strict requirement to establish a trust

by a written instrument⁷⁴. If the trust is reduced to writing, the instrument by which the trust is formed is called an ‘instrument of trust’ (s.3(2)).

Charitable or public trusts

858. Public charitable trusts (which also do not strictly require a written instrument to be formed) are designed to benefit members of an uncertain and fluctuating class. Depending on the corpus, a trust may be formed as a company or a society. In case of companies, section 25 of the Companies Act applies to non-profit making companies while institutions established for promoting religion, science, etc. may also be registered as limited companies. The federal Charitable and Religious Trusts Act, 1920 permits members of the public who have an interest in any charitable or religious trust to apply to a court to obtain an order directing its trustees to furnish information about the trust, including income and assets, and directing that the accounts of the trusts to be examined and audited. In addition, most States have enactments which govern their creation, administration and winding up – e.g. Bombay Public Trust Act, 1950 applicable in the States of Maharashtra and Gujarat. This Act provides for a Charity Commissioner to inspect and supervise the property belonging to a public trust registered under the Act, as well as the proceedings of the trustees and books of accounts of such a trust.

859. In general, charitable or public trusts may register for one or more of the following purposes:
- a. relief of poverty or distress;
 - b. education;
 - c. medical relief;
 - d. provision of facilities for recreation or other leisure-time occupation (including assistance for such provision), if the facilities are provided in the interest of social welfare and public benefit; and
 - e. advancement of any other object of general public utility, excluding purposes which relate exclusively to religious teaching or worship.

Wakfs

860. A “wakf” is a charitable Islamic trust that involves “the permanent dedication by a person professing Islam of any moveable or immoveable property for any purpose recognised by the Muslim law as pious, religious or charitable” and is governed by the Wakf’s Act, 1954. Through a written deed, the settlor appoints a manager for the administration of the wakf for certain property and once dedicated the trust is permanent, irrevocable and inalienable.

Tax issues related to the different categories of trusts

861. Trusts are not legal entities and are governed by the trust deed (if it exists) and applicable local laws. Under the Income Tax Act, 1961 wholly charitable and religious trusts are exempt from tax but this exemption must be granted by the tax authorities on application with information about the trustees and administration requirements of the trust. Private trusts are subject to taxation. Where tax on a discretionary trust is assessed in the hands of the trustee, after-tax distributions to the beneficiaries are exempt from tax in their individual hands. The trustee must file a tax return disclosing information about the income and assets of the trust he or she administers. However, generally, information about beneficiaries of the trust is not required to be filed.

⁷⁴ *Radha Soami Satsung Vs. CIT* - (1992) 193 ITR 321 (SC).

Central Registration System

Private trusts

862. Although not required by Indian law for private trusts, trust instruments (such as a trust deed) may be registered with a Sub-Registrar of Assurances under the Indian Registration Act, 1908 but a written instrument is not a strict requirement, and, as noted, there is no strict requirement to register. Indian authorities advised that no statistics are available on the number of private trusts in India, including those which voluntarily register with the Sub-Registrar of Assurances. Indian authorities indicated that most private trusts have a PAN number but could not provide statistics on those numbers.

Charitable and public trusts and wakfs

863. There are a variety of registration requirements for public or charitable trusts and wakfs in India, as indicated in the table below:

| Statute | Registration requirement |
|---|--|
| Societies Registration Act, 1860 | <ul style="list-style-type: none"> When a trust is constituted as a society, it is required to be registered under the Societies Registration Act. |
| State Public Trust Acts: e.g. Bombay Public Trust Act, 1950 | <ul style="list-style-type: none"> Public trusts to which this Act applies (public health, education relief of poverty) must register under s 18. |
| Income Tax Act, 1961 | <ul style="list-style-type: none"> Charitable or religious trusts, societies and companies claiming exemption under the Income-Tax Act ss.11 and 12AA are required to register under the Act. |
| Foreign Contribution (Regulation) Act, 1976 | <ul style="list-style-type: none"> Any charitable trust, society, company, desirous of receiving any foreign contributions from foreign sources, is required to register under section 6(1). |
| Companies Act, 1956 | <ul style="list-style-type: none"> A charitable institution/association can be registered as a non-profit company and obtain a licence under section 25. |
| Wakfs Act, 1954 | <ul style="list-style-type: none"> Every wakf created before or after the commencement of this Act must register at the Board. |

864. Indian authorities indicated that no statistics are available on the number of wakfs and charitable trusts.

Record-keeping and financial reporting requirements

865. For public and charitable trusts that are required to register (as stated above), the applicable statutes have requirements relating to the information that must be provided and filed annually with the various statutory authorities. Public trusts must also file annual budgets and financial reports which are independently audited (Wakfs Act ss.31, 50 51; Bombay Public Trust Act Chapter V), and maintain records for tax purposes.

866. For private trusts, section 19 of the Indian Trust Act requires trustees to “keep clear and accurate accounts of the trust-property, and at all reasonable times, at the request of the beneficiary, to furnish him with full and accurate information as to the amount and state of the trust-property” and to make those records available to a beneficiary for inspection (s.57). Where a private trust is required to file a tax return, it is a requirement of the Income-tax Act to maintain records for tax purposes.

Trust service providers

867. Indian law does not require those who perform trust services (primarily lawyers) to obtain, verify, or retain records on the beneficial ownership and/or control of trusts, or to retain copies of trust

instruments. Consequently, beneficial ownership information may not be available to competent authorities from these service providers.

Access to information by competent authorities

868. Law enforcement and other competent authorities have powers to obtain or access information held by the Sub-Registrar of Assurances, Charity Commissioner, Wakf Boards, Income Tax authorities and from the Ministry of Home Affairs or any State Government authorities in respect of these public charities. These records include registered trust deeds, accounts and financial statements. However, for private trusts, the record-keeping and financial information, including information about beneficiaries, is limited, if any. With respect to the latter, there is no specific provision in the Indian Trust Act that trustees maintain a register of ultimate beneficiaries. For instance, where a beneficiary of a private trust is a company, the trustee is not required to maintain information about the majority or minority shareholders of that company and so access by competent authorities to information, if any, held by trustees will be limited.

869. Although the authorities generally have sound investigative powers, information on beneficial ownership and control in relation to private trusts is generally not available to competent authorities since there is no obligation to obtain and retain it. Even trust deeds are generally unavailable since there is also no legal requirement on private trusts (or public trusts) to execute these instruments and when they are executed there is no legal requirement stipulating where trust deeds must be kept. Consequently, a trust deed may not generally be accessible by competent authorities, unless the trust has been registered.

Additional elements

870. There are no measures in place to facilitate access by financial institutions to beneficial ownership and control information beyond the immediate beneficial owner and immediate trustee, so as to allow them to more easily verify the customer identification data.

5.2.2 Recommendations and Comments

871. While India has some robust systems in place for public trusts (including record-keeping and maintenance of records, including financial records), measures relating to the collection of beneficial ownership information for private trusts is limited. India should further develop requirements to ensure that information on the beneficial ownership and control of private trusts is collected and readily available to the competent authorities in a timely manner. Such measures could include, for example, requiring trustees to maintain full information on the trust's beneficial ownership and control, requiring the location of such information to be disclosed, or requiring trust service providers to obtain and maintain beneficial ownership information. Such information would then be available to the law enforcement and other competent agencies upon the proper exercise of their existing powers.

5.2.3 Compliance with Recommendations 34

| | Rating | Summary of factors relative to s.5.2 underlying overall rating |
|-------------|---------------|--|
| R.34 | PC | <ul style="list-style-type: none"> • There is no requirement to obtain, verify and retain adequate, accurate and current information on the beneficial ownership and control of private trusts. • That are no measures in place that guarantee that minimal adequate and accurate information concerning the beneficial owners of private trusts can be obtained or accessed by the competent authorities in a timely fashion. |

5.3 *Non-profit organisations (SR.VIII)*

5.3.1 *Description and Analysis*

Special Recommendation VIII

872. Indian authorities have acknowledged significant risks for terrorist financing in the very large NPO sector. The NPO sector plays a vital social role in Indian society. India does not maintain a unified database for NPOs. Each registering authority maintains its own database. NPO registering authorities include a range of agencies for a variety of purposes:

- a. Ministry of Home Affairs (MHA) (Foreign Contributions (Regulation) Act, 1976 - FCRA);
- b. Income Tax Department (Income Tax Act);
- c. Registrar of Societies (Societies Registration Act);
- d. Charities Commissioner (Bombay Public Trust Act and other similar state statutes);
- e. Registrar of Companies (Companies Act) - s.25 not-for-profit companies.

Statistics on the number of registered NPOs under the various statutes are not generally available in India although the assessment team was advised that the Ministry of Home Affairs (MHA) (the registering authority for NPOs which involve the receipt and/or exchange of foreign currency) has probably the largest number of NPOs registered with it.

873. The Indian Planning Commission acts as an interface between the Government and the Indian NPO sector. It is not the Commission's role to register and/or regulate NPOs operating in India. However, NPOs doing business with the Indian Central Government must register specifically with the Commission in order to be able to do so. According to the "National Policy on the Voluntary Sector" published by the Planning Commission in 2007, the Central Government is committed to examining the feasibility of "enacting a simple and liberal Central law that will serve as an alternative all-India statute for registering the voluntary sector (*i.e.* NPOs), particularly those that wish to operate in different parts of the country and even abroad. Such a law would co-exist with prevailing Central and State laws, allowing an NPO the option of registering under one or more laws, depending on the nature and sphere of its activities". As of the date of the on-site visit, this Central law has not been enacted. Indian authorities provided no information on whether there is a similar registration requirement for NPOs wishing to do business with State Governments.

Size and characteristics of the NPO Sector in India

874. By government estimates, there are approximately 2 million foreign and domestic NPOs operating in India. NPOs seeking tax exempt status must register under the Income Tax Act. NPOs which receive funds from outside India must register under the FCRA. Indian authorities provided the following relevant statistics:

| | |
|--|-----------|
| Estimated total number of NPOs in India | 2 000 000 |
| Number of NPOs registered with the MHA under the FCRA | 38 591 |
| Number of NPOs that filed tax returns in the fiscal year 2006-2007 | 71 009 |

The authorities indicated that the number of tax returns stated above (71 009) represents the number filed in only seven Indian cities namely Delhi, Mumbai, Chennai, Kolkata, Bangalore, Hyderabad and Ahmedabad and advised that determining the total number of tax returns filed by NPOs across the entire country is not possible because those returns are intermingled with other Returns.

875. The total amount of foreign contributions by NPOs registered under the FCRA during the last five years is:

| Financial year | Foreign contributions reported (in million INR) |
|----------------|---|
| 2003-2004 | 5 105 500 |
| 2004-2005 | 6 256 680 |
| 2005-2006 | 7 877 570 |
| 2006-2007 | 11 336 970 |
| 2007-2008 | 9 663 460 |

876. There is no definition or classification of foreign NPOs under the FCRA. Foreign nationals are generally not permitted on the governing body of an association seeking registration or prior permission under the FCRA; however, a relaxation in this regard is considered on a case by case basis subject to certain conditions. Opening a liaison or branch office of foreign companies/associations in India, including NPOs, requires permission from the Reserve Bank of India under section 592 of the Companies Act.

Reviews of the domestic non-profit sector

877. India has not yet undertaken a review of its NPO sector as envisaged by the FATF standards. During the on-site visit, Indian authorities stated that NPOs are “monitored to ensure compliance” with legal requirements under various laws and “that domestic laws are periodically reviewed from time to time.” On the other hand, authorities agreed that this was a “day-to-day” business requirement of regulating agencies and that a comprehensive review of the NPO sector, including a risk assessment for possible abuse by terrorists, has not been undertaken. Nor is new information assessed or reviewed to determine the sector’s vulnerabilities to terrorist financing. In this regard, while a report entitled “Review of Indian NPO Sector” was submitted to the APG as part of the latter’s on-going NPO sector review programme, the report is perfunctory (3½ pages), lacking sufficient detail to meet the requirements of criterion VIII.1.

Outreach to the NPO sector concerning terrorist financing issues

878. There has been no effective outreach to the NPO sector by the Government of India or by State Governments in relation to risks and vulnerabilities of the sector to terrorist financing abuse. In the three years preceding the on-site visit, while some workshops were conducted to which NPOs were invited in order to enhance awareness among various stakeholders about the requirements under the Foreign Contribution (Regulations) Act and the Rules, only one workshop relating specifically to NPOs and FT risks was conducted - the South Asian Regional Conference on Combating Terrorist Financing in the charitable sector hosted by the US Embassy in New Delhi from 14-16 April 2009. This workshop was not attended by the private sector or NPOs but by representatives of SAARC countries and from India (officers of government agencies, including the Ministry of Home Affairs, the Central Bureau of Investigation, the FIU-IND, the Directorate of Enforcement, the Central Board of Direct Taxes, the SEBI, and others) and hence, this initiative does not qualify as outreach to the sector. Moreover, neither the Planning Commission (the primary agency for the sector) nor other government agencies or registering authorities have provided guidance or issued publications to the sector on the risks of terrorist financing in the sector.

Monitoring and sanctions

879. Except under the Income Tax Act and the FCRA, the NPO sector is subject to limited or no monitoring and supervision.

880. Under the Income Tax Act, the Tax Department reviews NPOs and their accounts only when the NPO seeks tax exempt status from the Commissioner; and when it files an annual tax return (including nil returns). This “review” is not for any other purpose but income tax compliance issues and authorities indicated during the on-site visit that only about 2% of the tax returns filed by NPOs is actually taken up for detailed examination on the basis of risk parameters. Under the FCRA, monitoring of receipt and utilisation of foreign contributions by NPOs is done through examination of audited annual returns. In case of any complaint or violations of the FCRA, an inspection of books of accounts and records of the associations is carried out and appropriate action is taken.

881. Apart from these activities (which are compliance based), authorities provided no other information on monitoring the activities of the sector. But even these activities are limited in light of the size of the sector. With 2 000 000 NPOs in India, only 38 591 are registered under the FCRA and a limited number of tax returns are discernable by authorities. It can therefore not be said that a “significant portion” of the financial resources of the sector and a substantial share of the international activities of the sector are being monitored.

882. If any association is found involved in misutilisation/diversion of foreign contributions, action is initiated against the association. Such action includes (i) placing the association in the “Prior Permission” category, (ii) prohibiting it from receiving foreign contributions, (iii) prosecuting it in a court of law, and (iv) freezing its bank accounts. In case of serious violations, where it is found that contributions are being diverted for purposes other than the stated objectives of the association, the matter is referred to the Central Bureau for Investigation for a detailed investigation and prosecution, if necessary.

883. Other than the MHA (for FCRA) and the Income Tax Department, there is no requirement for NPOs to be licensed or registered in India to conduct business as NPOs except under the Companies Act for section 25 not-for-profit companies.

884. Those NPOs which have tax exempt status in India are required to keep records of their transactions for tax purposes and for those registered under the FCRA for business purposes with the RBI. There is no information available to the Indian authorities concerning the large number of other NPOs that are not registered.

885. The following actions have been taken so far by the competent authorities where they identified irregularities by NPOs with respect to the following legislation:

- i. Under the Income Tax Act 1961:
 - a. the Income Tax department has issued notices in 652 cases over the last three years where NPOs had not filed their returns of income or had furnished incorrect particulars in their returns of income so filed;
 - b. penalties were imposed on NPOs in 721 cases under various sections of the Income Tax Act.
- ii. Under the FCRA:
 - a. 41 NPOs have been prohibited from receiving foreign contribution;
 - b. 4 NPOs have been placed in Prior Permission category;
 - c. accounts of 11 NPOs have been frozen;
 - d. 13 cases have been referred to CBI for detailed investigations for FCRA violations.

In addition, the CBI has registered cases against 16 NPOs in the period covering the financial year 2005-2006 to 2009-2010. No other information has been provided by India in relation to NPOs not registered with the tax department or under the FCRA.

Information gathering and investigation

886. NPOs are required to keep information on their purpose and objectives as well as ownership and control information. Information on ownership and control is however limited given the limited information required to be kept under general company law and the fact that no shareholder or members information for foreign companies or NPOs is required to be kept in India. What is recorded, however limited, is available to appropriate authorities.

887. India has legal provisions in the Code of Criminal Procedure (CrPC) and the Unlawful Activities (Prevention) Act (UAPA) to attach or freeze assets of a terrorist organisation or proceeds of terrorism. By exercising powers under sections 83 and 102 of the CrPC properties suspected to be involved or connected to crime or proceeds of crime, including on bank accounts, can be seized by the investigating agency. Further, section 12 of the FCRA empowers the Government to prohibit a person from paying, delivering, transferring or otherwise dealing in any manner with such article or currency, whether Indian or foreign, which is in his custody or control and has been accepted in contravention of any provision of FCRA.

Responding to international requests for information about an NPO of concern

888. The Ministry of Home Affairs (MHA) is the competent authority for receiving foreign requests for information, and therefore the responding agency for any international request for information regarding NPOs suspected of terrorist financing or other terrorist support. If the NPO is a registered entity, then details of it are available with the concerned registering authority and otherwise, information available is gathered through investigating agencies and shared with the requesting country.

889. As regards the exchange of information relating to criminal investigations, the CBI is the National Central Bureau and contact point for exchange of information with the foreign agencies. The CBI works closely with the other enforcement agencies of the country and makes the information requisitioned in criminal investigations available through the Interpol channel. India's Mutual Legal Assistance and extradition treaties provide additional exchange mechanisms (see Sections 6.3 and 6.4 for more details).

Implementation and effectiveness

890. Except for NPOs registered with the Income Tax Department and under the FCRA, India's NPO sector is not well organised, monitored and supervised. India concentrates most of its efforts on tax exempt NPOs as well as those receiving foreign contributions, but these NPOs only account for a small number of entities within the sector. While Indian officials indicated that they believe FT risk in the NPO sector is small, it is difficult to understand how they can maintain this confidence in light of the fact that they were unable to state the size, wealth and activities of the majority of NPOs in India.

5.3.2 Recommendations and Comments

891. It is recommended that India should:

- Undertake a comprehensive NPO sector review capturing all relevant data necessary, including the adequacy of domestic laws in the NPO sector.
- Undertake a detailed risk assessment of the sector for terrorist financing.

- Undertake comprehensive outreach to the NPO sector with a view to protecting the sector from abuse for terrorist financing as well as wider outreach in relation to good governance and accountability.
- Ensure that NPOs maintain information on the identity of the persons who own, control or direct their activities, including senior officers, board members and trustees.
- Demonstrate that appropriate measures are in place to sanction violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs, other than those registered under the Income Tax Act and the FCRA.
- Implement measures to ensure that all NPOs are licensed and/or registered as such and make this new information available to the competent authorities.

5.3.3 Compliance with Special Recommendation VIII

| | Rating | Summary of factors relative to s.5.3 underlying overall rating |
|---------|--------|---|
| SR.VIII | NC | <ul style="list-style-type: none"> • There is no review undertaken of the adequacy of domestic laws in the NPO sector. • There are no periodic reassessments undertaken by reviewing new information on the sector's potential vulnerabilities to terrorist activities. • There is no outreach to the NPO sector with a view to protecting the sector from abuse for terrorist financing takes place. • There is only limited information available on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. • India has not demonstrated that measures are in place to sanction violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs for NPOs other than those registered under the Income Tax Act and under the FCRA. • The majority of NPOs are not registered as such with government agencies, including the tax authorities. |

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 *National co-operation and co-ordination (R.31)*

6.1.1 *Description and Analysis*

Recommendation 31 (Domestic co-operation)

Policy co-operation

The Economic Intelligence Council (EIC)

892. The EIC has been established to enhance co-ordination between various enforcement agencies, intelligence agencies, regulators and departments in the Ministry of Finance (MOF) and the Ministry of Home Affairs (MHA). The EIC is the mechanism for national co-ordination among the various agencies involved in combating economic offences, including money laundering and terrorist financing. Its main purpose is to co-ordinate domestically concerning the development and implementation of policies and activities for AML and CFT. The EIC's mandate consists of the following elements:

- a. consider various aspects of intelligence relating to economic security and evolve strategy for effective collection and collation of such intelligence and its dissemination to identified user agencies and departments;
- b. review measures to combat economic offences and formulate a co-ordinated action strategy for the various enforcement agencies;
- c. review important cases involving inter-agency co-ordination and approve modalities for improving such co-ordination;
- d. consider and approve measures to strengthen the functioning of individual intelligence and enforcement agencies under the MOF;
- e. examine the changing dynamics of economic offences, including new modus operandi for such offences and approve measures for dealing with them effectively;
- f. advice on amendments of laws and procedures for plugging loopholes in taking effective action against economic offenders;
- g. review measures to combat the generation and laundering of illicit money and approve a strategy for dealing effectively with illicit money operators and tax evaders;
- h. interact through its secretariat, with the National Security Council Secretariat (NSCS) on matters having bearing on national and economic security;
- i. consider and approve lists of annual tasks, including the periodical updating of such lists, for each of the agencies concerned in consultation with the departments and agencies that finally receive the information, including the intelligence agencies, and make these task lists available to the NSCS;
- j. consider and introduce a system of annual monitoring and evaluation (qualitative and quantitative) of the performance (in the field of intelligence collection, prompt dissemination, follow-up etc.) of all agencies under its control;
- k. consider and suggest appropriate budgeting of all agencies under its control.

893. The EIC meets at least once a year, and in 2008, two such co-ordination meetings took place. During its meetings, the EIC discusses and takes decisions on issues pertaining to trends in economic offences, strategies on intelligence sharing, co-ordination, etc. A Working Group on Intelligence Apparatus

(WGIA) established within the EIC monitors the implementation of the decisions taken in the EIC meetings.

The Inter-Ministerial Co-operation Committee on Combating FT and Preventing ML (IMCC)

894. The IMCC was set up in 2002 pursuant to a decision of the Core Group on Security for the purpose of co-ordination, review and monitoring of action of regulators and enforcement agencies with regard to AML and CFT. The Co-ordination Committee is to act as policy maker to develop mechanism for:

- a. operational co-operation between the Government, law enforcement agencies, the FIU-IND and the regulators (RBI, SEBI and IRDA);
- b. policy co-operation and co-ordination across all relevant/competent authorities;
- c. consultation between the concerned authorities, the financial sector and other sectors, as appropriate, that are subject to AML/CFT laws, regulations, guidelines etc; and
- d. developing and implementing policies on AML/CFT.

895. The IMCC is chaired by the Additional Secretary of the Department of Economic Affairs and meets at least once in two months. Presently, it comprises of representatives from the Department of Economic Affairs (DEA), the Department of Revenue (DOR), the Ministry of Home Affairs (MHA), the Ministry of External Affairs (MEA), the Department of Financial Services (DFS), the Ministry of Law and Justice (MLJ), the Ministry of Company Affairs (MCA), the Directorate of Enforcement (ED), the Narcotics Control Bureau (NCB), the Directorate of Revenue Intelligence (DRI), the Central Economic Intelligence Bureau (CEIB), the FIU-IND, the RBI, the SEBI and the IRDA. Since February 2010, the Department of Posts has been added as a member in order to consolidate the position of India Post following its recent inclusion as a financial institution under the PMLA. The IMCC meetings generally focus on the review of the effectiveness of the AML/CFT regime so as to ensure that steps are taken to enhance AML/CFT measures. As a result of the IMCC's exercise, (i) the Unlawful Activities Prevention Act (UAPA) was amended in 2008; (ii) the Prevention of Money Laundering (PMLA) issued in 2002 came into force in 2005; (iii) the PMLA was amended in 2009, (iv) the PML Rules were amended in 2007, 2009 and 2010, and (v) the National Investigation Agency (NIA) was set up.

Operational co-operation

The Central Economic Intelligence Bureau (CEIB)

896. The CEIB was set up in 1985 and has the primary objective of providing operational co-ordination between the different enforcement and investigation agencies dealing with economic offences. To that extent, the CEIB has a mechanism of information exchange between the various agencies through the Group of Economic Intelligence (GEI), where so called *nodal* officers from various agencies collect information from their organisations and share it with the CEIB. It has also developed a database on economic offences and maintains files of significant offenders based on the inputs received from various agencies. In addition, the CEIB also interacts with the National Security Council Secretariat, the Intelligence Bureau, and the MHA on matters concerning national security and terrorism.

The Regional Economic Intelligence Committees (REIC)

897. At the field level there are 21 REICs set up as *nodal* agencies whose functioning is co-ordinated, supervised and monitored by the CEIB. The REICs meet every month and function similarly as the EIC. The REICs also organises zonal conferences for the agencies involved in the REIC concerned, where different problems and current issues are discussed and corrective steps are proposed.

The interdepartmental and interagency programmes

898. Several inter-departmental and inter-agency programmes are organised at various specialised institutions to develop skills and to improve co-ordination. During the financial year 2007-2008, the following special programmes were organised:

- a. prevention of insurance frauds at the National Insurance Academy in Pune;
- b. computer and internet crimes at the Sardar Vallabhbhai Patel Police Academy in Hyderabad;
- c. banking operations & fiscal law enforcement at the State Bank Staff College in Hyderabad;
- d. intelligence gathering & intelligence tradecraft at Military Intelligence Training School & Depot in Pune;
- e. intelligence gathering and intelligence tradecraft at the Intelligence Bureau's Central Training School in New Delhi.

Co-operation between regulatory authorities

899. At the national level, given the overlap in the activities of the banking, capital markets, insurance and pensions sectors, there is a formalised system of interaction of the RBI, the SEBI, the IRDA and the Interim Pension Fund Regulatory and Development Authority under the aegis of a High-Level Committee on Financial Markets, which meets at regular intervals.

Co-operation between the FIU and the LEAs; and the FIU and the regulators

900. The FIU-IND has put in place a mechanism that allows for the dissemination of cases to and the sharing of information and knowledge in relation to new developments in the field of AML/CFT with the LEAs and the regulators on a regular basis. This is ensured through frequent structured and unstructured meetings of the policy makers, regulators, and law enforcement authorities and includes sharing of information, organising workshops, training sessions, etc. In addition, on 24 December 2009, the FIU-IND has appointed a system integrator for setting up an advanced technical infrastructure under its project FINnet to enable secure operational co-operation with the law enforcement agencies and the regulators. The FIU, law enforcement agencies and the regulators regularly interact on various forums on policy co-ordination issues.

Additional elements

901. The policy makers, regulators and FIU have separate mechanisms in place for involving the financial sector and other relevant sectors in their consultation processes. In view of ensuring compliance with the obligations under the PMLA, the FIU-IND works closely with the respective regulators and industry. The relevant *nodal* officers at the FIU-IND interact with the principal officers of the reporting entities on a regular basis to assess the effectiveness of their AML/CFT systems and to provide them feedback and guidance (see Section 3.7 above for more details in this regard).

Implementation and effectiveness

902. There are several mechanisms in place to ensure operational co-operation. Inter-agency co-ordination and co-operation appears to be imbedded in the Indian system, having been mandated by the Central government, not just for AML purposes but for a range of other activities, including national security. The following example cited by the authorities during the on-site visit shows that overall the agencies inter-act well at the operational level: the Punjab State Police advised the assessment team that the Directorate of Enforcement (ED) has 40 staff located in Chandigarh, and provided specific case studies to show how they worked alongside the ED staff. In practice, the mandated co-operation between agencies was supported by comments received from the agencies present during the discussion with Punjab State Police. In addition, the Uttar Pradesh State Police reinforced these comments. As indicated in Section 2.6

above, the PMLA (s.54(f)) empowers and requires police officers to assist authorities with the enforcement of the PMLA.

903. In terms of parallel ML and predicate offence investigations, the assessment team received assurances from the ED about its ability to gather evidence and work alongside the agency responsible for the predicate offence investigation. The increase in the number of registered cases through 2009 certainly supports this position. So far, there are only six prosecutions for money laundering and no convictions (see also Section 2.1 of this report). Pending convictions that illustrate the ability to effectively gather evidence and prosecute money laundering in separate proceedings, the effectiveness of the domestic co-ordination and co-operation mechanisms in place has not yet been demonstrated.

Recommendation 30 - Resources of policy makers

904. The Ministry of Finance is the policy maker with respect to AML measures, while both the MHA and the MOF are policy makers with respect to CFT measures. The Indian authorities report that the MHA and the MOF are adequately structured, funded and staffed, and have sufficient technical and other resources in order to perform their functions effectively.

905. Officers responsible for AML/CFT policy making in the relevant Ministries are from the Indian Administrative Services, the Indian Revenue Services, the Indian Police Services and from other All India Civil Services. The Indian authorities report that all officers and staff members of the policy makers maintain high professional standards, including standards of confidentiality, high integrity and are appropriately skilled. All the civil servants are subject to strict disciplinary and conduct Rules. The professional standards of the staff of the FIU-IND, the law enforcement authorities and the supervisory authorities are set out extensively in sections 2.5; 2.6; and 3.10 respectively.

906. The officers of the policy-making ministries have participated in training courses, such as FATF/APG assessor trainings, and regularly attend FATF and APG Plenary and Working group meetings.

Recommendation 32 - Reviewing the effectiveness of AML/CFT regimes

907. There are several systems in place for the regular review of the effectiveness and functioning of India's AML/CFT system. The Economic Intelligence Council, chaired by the Finance Minister of India, conducts periodical reviews at the national level regarding both the effectiveness of the legal framework and the processes in place by law enforcement agencies. The CEIB and the REIC also organise regular review meetings to discuss and examine strategies including the assessment of the efforts to combat money laundering and terrorist financing. The Revenue Secretary regularly reviews the functioning and effectiveness of both the Directorate of Enforcement and the FIU-IND.

908. The Inter-Ministerial Co-ordination Committee on Combating Financing of Terrorism and Prevention of Money Laundering (IMCC) reviews the effectiveness of the systems for AML/CFT on a regular basis and ensures that steps are taken to update AML/CFT measures, as necessary. As a result of such exercises, the UAPA and PMLA have been amended and the National Investigation Agency has been set-up under a separate statute to investigate and prosecute terrorists involved in terrorist activities, including terrorist financing.

6.1.2 Recommendations and Comments

909. While India has initiated a large number of ML investigations (798 at 31 December 2009), only six prosecutions are underway and there are no convictions so far. India has yet to achieve convictions and additional prosecutions that demonstrate the effectiveness of its inter-agency co-ordination and co-operation.

6.1.3 Compliance with Recommendation 31

| | Rating | Summary of factors relative to s.6.1 underlying overall rating |
|------|--------|---|
| R.31 | LC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ the effectiveness of the inter-agency co-ordination and co-operation has not yet been demonstrated. |

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Recommendation 35 and Special Recommendation I

United Nations Conventions

Money Laundering

910. India acceded to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) on 27 March 1990. The United Nations Convention against Transnational Organised Crime (Palermo (TOC) Convention) was signed on 12 December 2002, but ratification is still pending.

911. Most of the Conventions' provisions, including the TOC Convention, have been implemented, mainly through the NDPS Act, 1985 and the PMLA, 2002, as amended. The international co-operation and extradition aspects are adequately covered by the Code of Criminal Procedure (CrPC) and the Extradition Act, 1962. However, as noted under Sections 2.1 and 2.3, the implementation of the criminalisation of the ML provisions and the seizure/confiscation regime show some critical deficiencies in that:

- the conduct of concealment, acquisition, possession and use of criminal proceeds are not (fully) covered by the PMLA (Art. 3(b)(ii) and (c)(i) of the Vienna Convention; Art. 6.1(a)(ii) and (b)(i) of the TOC Convention);
- the seizure/confiscation regime of the laundered proceeds is restricted (Art. 5 of the Vienna Convention; Art. 12 of the TOC Convention);
- the sanction for drug related ML under the NDPS Act is not consistent (Art. 4(a) of the Vienna Convention);
- the fines imposable on legal persons are not consistent (Art. 10.4 of the TOC Convention);
- in general, the effective implementation of the ML provisions is a matter of concern in view of the absence of ML convictions.

912. Furthermore, the regulatory and supervisory regime is not fully and effectively implemented, as noted in Sections 3 and 4 of this report (Art. 7.1(a) of the TOC Convention calls for a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions ... which regime shall emphasise requirements for customer identification, record-keeping and the reporting of suspicious transactions).

Terrorist Financing

913. India signed the International Convention for the Suppression of the Financing of Terrorism (FT Convention) on 8 September 2000 and submitted the instrument of ratification on 22 April 2003. The UAPA, 1967, as amended, is the main domestic implementing legal instrument.

914. As noted under section 2.2 of this report, the UAPA deviates from the FT Convention on several points:

- the criminalisation of the financing of the offences falling within the scope of the Treaties annexed to the FT Convention is not consistent and not all relevant offences are covered (Art. 2.1(a) of the FT Convention);
- the law does not cover the threat to international organisations (Art. 2.1(b) of the FT Convention);
- the terrorist financing attempt is only partially criminalised (Art. 2.4 of the FT Convention);
- the confiscation of funds to be used by terrorist individuals is problematic (Art. 8 of the FT Convention);
- the preventive measures imposed by Art. 18.1 and 2 of the FT Convention are not fully and effectively implemented, as noted under Sections 3 and 4 of this report;
- general effectiveness concerns in view of the minimal number of convictions and absence of firm jurisprudence.

United Nations Resolutions

915. With the UAPA, as amended, India has implemented the S/RES/1267(1999), its successor resolutions, and S/RES/1373(2001). The implementation is however affected by some technical deficiencies, as noted in Section 2.4 above.

Additional elements

916. India is a signatory to all 13 terrorism related UN Conventions. India is a Member State of the South Asian Association for Regional Co-operation (SAARC) and ratified the said SAARC Regional Convention on the Suppression of Terrorism.

917. The SAARC Additional Protocol to the SAARC Regional Convention on the Suppression of Terrorism, recognising the importance of updating the Convention, in order to meet the obligations devolving in terms of Security Council Resolution 1373, was signed by India on 6 January 2004.

6.2.2 Recommendations and Comments

918. Besides ratifying the Palermo Convention⁷⁵, India should review its ML and FT provisions to bring them in line with the relevant Conventions, particularly in respect of the criminalisation and the implementation of the preventive regime.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

| | Rating | Summary of factors relative to s.6.2 underlying overall rating |
|------|--------|--|
| R.35 | PC | <ul style="list-style-type: none"> • Palermo TOC Convention not ratified. • Criminalisation of ML not in line with the Vienna and TOC Conventions (concealment, acquisition, possession and use). • Restricted ML seizure/confiscation regime. • Inadequate sanctions for the ML offence in the NDPS Act and the sanctions for legal |

⁷⁵ The Union Cabinet of India in its meeting held on the 19 March 2010 has approved the ratification of the Palermo Convention. India is in the process to complete the necessary formalities.

| | Rating | Summary of factors relative to s.6.2 underlying overall rating |
|-------------|-----------|--|
| | | <p>persons in the PMLA.</p> <ul style="list-style-type: none"> • Deficiencies in the regulatory and supervisory regime. • Effectiveness issue: <ul style="list-style-type: none"> ○ absence of convictions. |
| SR.I | PC | <ul style="list-style-type: none"> • FT criminalisation not in line with the FT Convention (FT offences, international organisations, attempt). • Confiscation of terrorist funds is deficient. • UN RES are not fully implemented. • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns regarding preventive regime and judicial follow-up in terms of final convictions. |

6.3 *Mutual Legal Assistance (R.36-38, SR.V)*

6.3.1 *Description and Analysis*

919. The statutory provisions for mutual legal assistance in criminal matters, including money laundering and terrorist financing, are contained in the following statutes:

- a. the Code of Criminal Procedure;
- b. the Extradition Act 1962; and
- c. the PMLA, 2002.

The relevant provisions of the Code of Criminal Procedure (CrPC) for Mutual Legal Assistance (MLA) are section 166B (Chapter XII), Chapter VII and Chapter VIIA. Chapter IX of the PMLA also confers powers on authorities/courts to provide MLA to contracting countries.

920. In addition, India can render assistance under a Mutual Legal Assistance Treaty (MLAT) which it has concluded with 26 countries (contracting States) and a further five are being finalised. Requests for assistance can be executed even where there is no MLAT with other countries on the basis of an assurance of reciprocity. India is also a party to international Conventions and agreements containing MLA provisions. India can act upon MLA requests through those provisions where there is no specific MLAT with the requesting or receiving country.

Procedure for incoming request for MLA and agencies involved

921. The following agencies are involved in India's MLA process:

- a. the Ministry of External Affairs (MEA);
- b. the Ministry of Home Affairs (MHA);
- c. the Department of Revenue (DOR);
- d. the International Police Co-operation Cell (IPCC) of the CBI in New Delhi;
- e. the Central Bureau of Investigation (CBI);
- f. the Directorate of Enforcement (ED);
- g. the Narcotics Control Bureau (NCB);
- h. the State Police;

i. the Customs/Directorate of Revenue Intelligence (DRI).

922. MLA requests in general, and in relation to money laundering in particular, usually come to the Central Government via diplomatic channels and are then passed on to the relevant court or law enforcement agency. The procedure is as follows: in general, the MHA, as the Ministry responsible for counter-terrorism and in charge of overseeing law enforcement and security matters, receives the requests for MLA. The CBI in New Delhi co-ordinates execution of such requests, on behalf of the MHA, through its own offices or through the State Police agencies. Requests related to ML are executed by the ED. If a MLAT or other previous arrangement is in place, it will specify the procedure to be taken to request assistance. Otherwise, action is taken on the basis of assurance of reciprocity.

923. In respect of MLA requests pertaining to ML, section 55(a) of the PMLA defines “contracting State” to mean *any country or place outside India in respect of which arrangements have been made by the Central Government with the Government of such country through a treaty or otherwise*. The phrase “otherwise” covers arrangements entered into on the principle of reciprocity.

924. The legal basis to provide MLA on the basis of reciprocity for FT and other offences is covered in section 105A(a) of the CrPC which also defines the term “contracting State” as *any country or place outside India in respect of which arrangements have been made by the Central Government with the Government of such country through a treaty or otherwise*. The phrase “otherwise” also covers arrangements entered into on the principle of reciprocity.

925. The requests are executed under the provisions of the Indian laws, as applicable. After execution, the investigating agency forwards the report to the CBI in New Delhi along with the evidence and material collected. In case of ML requests, the ED forwards the material collected to the requesting authority through the MEA. The file is then forwarded to the Central Authority of the requesting country through the MEA under intimation to the MHA.

Recommendation 36 and Special Recommendation V (Mutual legal assistance)

Range of mutual legal assistance available

926. The MLA provisions in the PMLA allow for a broad range of assistance to be provided in ML cases, either pursuant to a formal agreement or on a reciprocal basis (ss.55 and 56 of the PMLA). For contracting States, the production, search, seizure of documents and taking of witness statements, service of documents, the tracing and identifying of property and attachment and confiscation of property is provided for in accordance with sections 59 and 60 of the PMLA.

927. India can also provide a wide range of assistance under section 105 and Chapter VIIA of the CrPC for FT investigations and prosecutions for contracting States. This includes warrants for arrest, to attend court or produce a document (s.105B (3)), attachment or forfeiture (s.105C(3)), tracing and identifying proceeds of crime (where there is an attachment or forfeiture order) (s.105D(1)), seizure (where there is an attachment or forfeiture order) (s.105E(1)). Section 166B provides for assistance for all countries in examination of any person or production of any document or thing in relation to an offence under investigation.

928. The MEA has issued instructions for handling MLA requests on 24 September 2007. In addition, the MHA has issued guidelines for investigations abroad related to MLA requests on 31 December 2007 and guidelines regarding summons/notices/judicial processes to apply to persons residing abroad on 11 February 2009. The DRI has also issued detailed guidelines on 21 April 2008 prescribing the procedure for handling MLA requests related to ML cases. To facilitate the execution of MLA requests received from competent authorities in foreign jurisdictions and to minimise the time of processing and execution such

requests, a Technical Circular has been issued on 16 March 2009 by the ED taking into consideration various instructions from the Ministry of Finance on the subject. According to the statistics available, the average turnaround time for incoming requests on MLA has been 6-7 months during the last three years in comparison with three months during 2009.

Prohibitions and conditions

929. India places few conditions or restrictions on the application of its mutual legal assistance provision. The CrPC does not provide any conditions under which a request would be refused. Any conditions that are imposed would be contained in the MLAT itself. While it is at the discretion of the Central Government whether to pass a request on to the CBI (CrPC s.166B), the assessment team was informed that, in practice, MLA requests are rarely refused. Assistance is refused only if the execution of the request would impair sovereignty or is against the national interest or the execution of the request is contrary to domestic law. A total of 30 incoming requests have been rejected since 2006. The most important reasons for rejection of a MLA request have been lack of assurance of reciprocity; the request did not pertain to India; no English translation; and absence of an explanatory letter. Normally the issue is taken up with the requesting country to address the deficiencies. All requests accepted receive a response, even if they come through informal channels. There is no fiscal exemption: in one specific case, a letter of request involving fiscal law offences has been executed and evidence was transmitted to the requesting country.

930. Similarly, the PMLA does not provide any conditions under which a request would be refused. Under the PMLA, the Central Government has discretion over whether to pass on a request to the relevant court or law enforcement agency (PMLA s.58) but that discretion must be exercised as it thinks fit in accordance with the PMLA or other laws. In other words, it is not unfettered discretion but must be exercised under a law to give effect to the request.

931. Secrecy or confidentiality requirements observed by financial institutions or DNFBPs do not constitute a legal ground for refusal of a MLA request. In practice, letters of request have been executed and details were obtained from financial institutions and provided as evidence to the requesting State.

Powers of competent authorities when executing mutual legal assistance requests

932. All the powers that are available for domestic ML cases are also available for MLA requests according to sections 17 and 18 of the PMLA while such relevant powers in relation to FT cases are available through Chapter VIIA and section 166B of the CrPC.

933. Terrorist acts and terrorist financing have been criminalised under the UAPA (see Section 2.2 above), and all offences under the UAPA are investigated, prosecuted, and otherwise dealt with according to the provisions of the CrPC (unless otherwise provided in the UAPA). These provisions allow for a wide range of MLA and the processes for providing such assistance have been detailed in the administrative guidelines mentioned above.

Conflicts of jurisdiction

934. The determination of the best venue for prosecutions, where prosecution would be possible in more than one jurisdiction, is settled on a case-by-case basis, through diplomatic channels. The Government would examine such request taking into consideration circumstances such as, place of commission of the offence, the gravity of the offence and the place where the witnesses and evidences are available. No such conflict of jurisdiction has arisen in relation to any foreign country.

Additional elements

935. The powers of competent authorities to (a) compel production of; (b) search persons or premises for; and (c) seize and obtain transaction records, identification data, account files and business correspondence and other records, documents, or information, held or maintained by financial institutions and other businesses or persons are also available when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts. Section 166B of the CrPC allows that upon receipt of a MLA request from a court or a competent authority in any country or place outside India in relation to the investigation of an offence, the matter shall be investigated in the same manner as if the offence had been committed within India. However, the MLA request is to be made through the Central Government.

Recommendation 37 and Special Recommendation V (Dual criminality relating to MLA)

936. Section 166B of the CrPC allows for assistance to be provided where there is “an offence under investigation” in another country, without formally imposing dual criminality as a condition for MLA. There is a test of dual criminality, but, in general, it is not strictly applied. However, if a foreign country, while negotiating a MLAT with India, makes dual criminality a mandatory requirement, that would be equally applicable in respect of both countries. Indian authorities confirmed that as a rule, technical differences in the offences are not viewed as an impediment. MLA requests requiring coercive measures requiring a court decision, however, are not viewed with the same flexibility: there is (at least) one case on record where a request for seizure was denied by the court on the ground that the alleged criminal conduct did not constitute an offence in India.

937. The provisions of the CrPC provide for mutual legal assistance in the absence of dual criminality and these apply equally for FT offences. However, the principle of dual criminality becomes relevant if the MLAT specifically makes such provision. As with ML, as a rule, formal or technical differences in the manner in which each country categorises or denominates the offence do not pose an impediment to the provision of assistance, unless there is a provision to the contrary in the relevant MLAT or other bilateral arrangement.

Recommendation 38 and Special Recommendation V (MLA – Freezing, seizing and confiscation)

Money laundering

938. India can provide assistance to requests for tracing, identification and attachment of property derived or obtained from the commission of an offence committed in the requesting State. The assistance would also include instrumentalities used in an offence if it is covered in a MLAT and available under domestic law. Section 60(6) of the PMLA allows for the search, seizure, attachment and confiscation provisions of the Act to be used in MLA cases. However, the domestic legal issues on the possibility to confiscate property laundered and proceeds of ML offences also impact on the capacity for India to provide such form of assistance (see Section 2.3 above for more details in this regard).

939. Section 105A(c) of the CrPC defines proceeds of crime including value of any property and section 105H of the CrPC allows the court to specify to the best of its ability which properties are proceeds of crime, where it is not possible to identify the exact proceeds. This covers the proceeds from terrorist activities and terrorist financing, not the funds or assets serving to finance those activities. As mentioned in Section 2.3 above, the definitions of proceeds of crime and property in the PMLA are broad enough to allow for confiscation of corresponding value. However, confiscation is only possible when there is a conviction of a scheduled (predicate) offence and only proceeds of the predicate offence can then be confiscated. As also stated in Section 2.3 above, property of corresponding value cannot be confiscated under the UAPA and the NDPS Act, except in limited circumstances. These shortcomings also affect the possibilities to provide MLA.

Terrorist Financing

940. Chapter VIIA of the CrPC provides for MLA regarding identification, seizure or forfeiture of proceeds of crime and assets actually used in the commission of an offence, including property obtained through proceeds of crime. This means that proceeds and instrumentalities used in a FT offence are covered. Confiscation of intended instrumentalities to be used by a terrorist individual are however not covered. Property of corresponding value is covered by the definition of proceeds of crime in section 105A of the CrPC which mirrors the PMLA definition. However, since the UAPA provisions do not cover corresponding value, the capacity to provide MLA is limited in this respect.

Co-ordination

941. India has MLATs with 26 contracting States, which provide for co-ordinating seizure and confiscation actions with other countries. As for the rest, it is a matter of operational practice for the competent judicial and law enforcement authorities to co-ordinate their actions with their foreign counterparts.

Assets forfeiture funds and sharing of assets

942. Forfeited assets vest with the Central Government and are credited to the Consolidated Fund of India. India being a welfare State, public expenditure on health, education, poverty alleviation, rural employment, infrastructure development, etc. is incurred from the Consolidated Fund. Further, the Fund is also used to attribute compensation to the victims of terrorism by the concerned State Governments.

943. Since the 2009 amendment to the PMLA, India is in a position to share assets confiscated as a result of the execution of a request from a contracting State (PMLA s.60(7)). To the extent that the proceeds of terrorism are confiscated under the provisions of the PMLA, the same provision applies for the sharing of confiscated assets with another country. So far, no request from any country has been received in this respect.

Additional elements

944. In general, Indian law only provides for the confiscation of the proceeds of crime when there is a criminal confiscation order. Even though it is possible to conduct a non-criminal confiscation in accordance with section 24(2) of the UAPA and Chapter VA of the NDPS Act, which provides a method of non-conviction based forfeiture of illegally acquired properties relating to trafficking of drugs, India cannot recognise a foreign request based on a non-criminal confiscation order only.

Recommendation 30 - Resources (authorities involved in MLA)

945. The MHA, the MEA, the DOR, the ED, the CBI and the State Police agencies, involved in dealing with MLA and extradition requests, appear to be well structured. The ED, the CBI and the State Police have operational independence and autonomy, are adequately funded and have adequate technical support to perform their functions.

946. The officers of the MHA, the MEA, the DOR, the ED, the CBI and the State Police are government servants and work as per standard operating procedures. They are required to observe integrity and confidentiality and maintain professional standards based on their respective conduct rules.

947. The officers and staff of the law enforcement agencies are provided with training, which also includes awareness raising regarding raising, collecting, and providing funds for terrorist activities and the measures implemented to combat terrorist financing. The training programmes equally focus on ML trends and techniques (see also Section 2.6 in this regard).

Recommendation 32 - Statistics

948. The table below gives an overview of the outgoing MLA requests for the period 2006-2009. It is indicated how many of these request relate to FT offences.

Statistics: Mutual legal assistance- All outgoing requests

| | 2006 | 2007 | 2008 | 2009 As on 31.12.2009 |
|---|--|--|--|--|
| Outgoing requests | 30 (145 earlier pending) | 41 (160 previous year pending) | 38 (186 previous year pending) | 50 (240 previous year pending) |
| Acceded requests | 26 | 37 | 32 | 50 |
| Rejected requests | - | - | 4 | - |
| Partially acceded requests | 4 | 4 | 2 | - |
| Executed requests | 15 | 15 | 10 | 19 |
| Withdrawn requests | - | - | - | 6 |
| Pending requests | 160 (including 142 requests for other offences and 18 requests for terrorist offences) | 186 (including 168 requests for other offences and 18 requests for terrorist offences) | 210 (including 193 requests for other offences and 17 requests for terrorist offences) | 245 (including 226 requests for other offences and 14 requests for terrorist offences) |
| Requests deemed lapsed | - | - | - | - |
| Requests for ML offences | - | - | - | - |
| Requests for other offences . | 142 | 168 | 193 | 226 |
| Requests for terrorist related offences | 26 | 19 | 18 | 18 |
| Status | | | | |
| Acceded | 8 | 1 | 1 | 4 |
| Rejected | - | - | - | - |
| Pending | 18 | 18 | 17 | 14 |

Statistics: Mutual legal assistance – outgoing requests with regard to ML

| | Name of country | No. of LR sent | Status |
|--------------|-----------------|----------------|---|
| 1. | Australia | 1 | Reply awaited |
| 2. | Hong Kong | 2 | Reply awaited |
| 3. | Switzerland | 1 | Partly reply received and matter is in progress |
| 4. | United Kingdom | 1 | Reply awaited, reminder issued |
| 5. | Canada | 1 | Reply awaited |
| 6. | Netherlands | 1 | Reply awaited |
| Total | | 7 | |

949. The Indian authorities state that the average turnaround time for mutual legal assistance or other international requests for co-operation for MLA that are made to foreign countries by India comes to approximately three years five months and 13 days. As regards the outgoing requests for MLA, out of the pending requests, during 2009, 18 related to terrorism out of which one related to a FT case.

Statistics: Mutual legal assistance – All incoming requests

| | 2006 | 2007 | 2008 | 2009 |
|--|--|--|--|--|
| Incoming requests | 32 | 39 | 45 | 27 |
| Incoming requests by Heads of assistance | - | - | - | - |
| Acceded requests | 20 | 26 | 42 | 23 |
| Rejected requests | 12 | 11 | 3 | 4 |
| Partially acceded requests | - | - | - | - |
| Withdrawn requests | - | 2 | - | - |
| Executed requests | 19 | 19 | 21 | 03 |
| Pending requests | 1 (all remaining MLA requests have been executed by various law enforcement authorities) | 7 (all remaining MLA requests have been executed by various law enforcement authorities) | 21 (all remaining MLA requests have been executed by various law enforcement agencies) | 20(all remaining MLA requests have been executed by various law enforcement authorities) |
| Requests deemed lapsed | - | - | - | - |
| Requests for other offences . | 27 | 30 | 38 | 9 |
| Average turnaround time | 7 months | 7 months | 6 months | 3 months |
| Requests for terrorist related offences | - | 2 | 1 | 1 |
| Status (acceded/rejected /pending) | - | 1 executed 1 pending | 1 executed | Certain clarifications sought from concerned authorities |

Statistics: Mutual legal assistance – incoming requests with regard to ML

| . | Name of country | No. of LR received | Status |
|--------------|-----------------|--------------------|--|
| 1. | Jersey Island | 2 | One LR Executed and reply sent. Another was withdrawn by Requesting Country. |
| 2. | UK | 3 | Two under execution, visit by officials of Requesting country is awaited. |
| 3. | Belgium | 1 | Under execution. Visit of foreign officials awaited. |
| 4. | Netherland | 1 | Executed and evidences sent. |
| 5. | USA | 1 | Under examination |
| 6. | Malaysia | 1 | Executed |
| Total | | 9 | |

950. With regard to the incoming requests for MLA, the four cases that refer to terrorist related offences were related to terrorist activities in general and not to terrorist financing. The cases involved inter alia: to provide information pertaining to an arrested terrorist; to interview and take a statement in writing from witnesses; to examine telephone records; to establish employment records, contacts, venues visited

and associates; to provide intelligence, information and assistance to the police of the requesting country; and to examine persons arrested in India. The nine ML cases involved collection of evidence, recording statement and seizure of proceeds of crime.

Implementation and effectiveness

951. India provides mutual legal assistance on the basis of MLATs with contracting States, treaties containing MLA provisions and requests for assistance based on reciprocity. There are provisions for MLA with contracting States in the PMLA and the CrPC. MLA with other countries is considered on an *ad hoc* basis (PMLA s.55 read with s.56(1) and CrPC. ss.105A(a), 166B).

952. There are few conditions or restrictions on the provisions of MLA. A request is not refused on the sole ground that the offence involves fiscal matters or that it imposes secrecy or confidential requirements on financial institutions or DNFBPs.

953. The possibilities to provide MLA in relation to coercive measures are however limited by the deficiencies in the criminalisation of ML/FT and the domestic framework of confiscation and provisional measures (see Section 2 above). In particular, the fact that it is not possible in the domestic context to confiscate laundered property or proceeds from ML offences and instrumentalities to be used by an individual terrorist also constitutes a legal obstacle to confiscate such property/proceeds in the international context. The same problems occur with dual criminality requirements in relation to MLA. One case is on record where MLA was refused by the court because the act was not criminalised in India.

954. There has been only one outgoing request for MLA concerning terrorist financing and seven outgoing requests request on MLA concerning money laundering. There were nine incoming requests on MLA related to money laundering and no incoming request for MLA concerning terrorist financing. India has reported an average turnaround time for incoming requests on MLA amounting to six to seven months and for the last year only three months. There are however some countries who have encountered problems with international co-operation via formal legal channels with India. The problems reported relate to the delay in the Indian authorities' reaction when providing MLA, if MLA is provided at all.

6.3.2 Recommendations and Comments

955. Although there are measures in place in the laws to provide mutual legal assistance in criminal matters and structured mechanisms for handling such requests, some shortcomings still exist. First of all, it is recommended that India gives high priority to providing MLA in a timely manner. Secondly, by addressing the identified legal deficiencies, the capacity for India for MLA would automatically be enhanced. The Indian authorities should therefore rectify domestic shortcomings regarding criminalisation, confiscation and provisional measures, which also affect the possibilities to provide MLA in coercive actions.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

| | Rating | Summary of factors relevant to s.6.3 underlying overall rating |
|------|--------|--|
| R.36 | LC | <ul style="list-style-type: none"> • MLA in coercive actions may be hampered as a result of domestic legal deficiencies (dual criminality). • Effectiveness issue: <ul style="list-style-type: none"> ◦ India does not provide MLA in a timely manner. |
| R.37 | LC | <ul style="list-style-type: none"> • MLA in coercive actions may be hampered as a result of domestic legal deficiencies (dual criminality). |
| R.38 | LC | <ul style="list-style-type: none"> • Deficiencies in confiscation regime of laundered property, instrumentalities and proceeds of money laundering affect the MLA capability. |
| SR.V | LC | <ul style="list-style-type: none"> • MLA in coercive actions may be hampered as a result of domestic legal deficiencies (dual criminality). • Deficiencies in the confiscation regime related to FT affect the MLA capability. |

6.4 Extradition (R.37, 39, SR.V)

6.4.1 Description and Analysis

Recommendation 39 and Special Recommendation V (Extradition)

956. Money laundering and terrorist financing are extraditable offences under the provisions of the Extradition Act (s.2(c)). Where an extradition treaty is in place with a foreign State, money laundering and terrorist financing are extraditable offences if it is provided for in the treaty. In relation to foreign States, other than treaty States, extraditable offences under the Extradition Act require a punishment of imprisonment of one year or more. Both the ML offence under the PMLA and the FT offence under the UAPA fall in that category, as they are punishable with imprisonment for a term not less than three and five years respectively.

957. In order to comply with an extradition request, India requires there to be a bilateral treaty or extradition arrangement with the requesting country or both countries to be party to an international treaty that contains extradition provisions. India has signed extradition treaties with 31 countries, is under various stages of negotiations with a further 31 countries, and has other extradition arrangements in place with nine countries. India is also a party to regional extradition treaties such as the London Scheme. Where there is no extradition treaty between India and any foreign State, the Central Government may, by notified order, treat any Convention to which India and a foreign State are parties, as an extradition treaty made by India with that foreign State providing for extradition in respect of the offences specified in that Convention (Extradition Act s.3(4)).

958. It is possible for India to extradite for money laundering and/or terrorist financing at the request of a country that is not party to a bilateral treaty or a Convention, purely on an *ad hoc* basis (Extradition Act ss.2(c)(ii) and (f) and 3(1)). A request for extradition of a fugitive criminal, which means a person who is accused or convicted of an extraditable offence within the jurisdiction of a foreign State, could be considered, in the absence of a bilateral treaty or any applicable convention, by notifying the foreign country concerned as a reciprocating country under the Extradition Act, provided the alleged conduct of the fugitive criminal amounts to an extraditable offence under Indian laws. As a matter of policy, it is however a condition that the foreign country concerned will also have to consider Indian requests for extradition. In such cases, the procedure governing extradition proceedings would also be as prescribed in the Extradition Act and laws of the respective countries in the absence of a negotiated treaty.

959. There is no bar to the extradition of Indian citizens. With a treaty State, the implementation of the provisions of the Extradition Act is governed by the treaty provisions in this regard. In case an Indian citizen is not extradited, the Act provides for his prosecution in India and the proceedings are conducted in the same manner as in the case of any other offence of a serious nature under the domestic law (Extradition Act s.34A).

960. Where a fugitive criminal is not extradited but is prosecuted in India, the Extradition Act provides for the receipt in evidence of the duly authenticated exhibits, depositions and other documents submitted by the requesting State (Extradition Act s.10). In addition, co-operation in obtaining evidence and securing transfer of persons and seizure and attachment of property is provided for in the CrPC.

961. Requests for extradition generally arrive through diplomatic channels, and are then transferred to the MEA who will examine the request, appoint an extradition magistrate and direct him to inquire into the case. The time taken to deal with extradition requests can vary largely. If the person surrenders, the case can be fast tracked and dealt with very quickly. However, India also indicated that dealing with extradition cases could take from 6 months to one year. An explanation for that can be found in the fact that

extradition cases can pass through three levels of court proceedings – the Magistrates Court, the High Court, and the Supreme Court.

Additional elements

962. Simplified procedures for extradition are in place, and allow for direct transmission of requests between appropriate Ministries (Extradition Act s.4) and the Indian authorities state that such simplified procedures are also applicable for terrorist and FT offences. The provisions for extradition based only on warrants of arrest or judgments, and extradition of consenting persons who waive formal extradition proceedings, exist in Chapter III of the Extradition Act. These provisions are only applicable to those treaty States in respect of which the treaty provides for the application of the simplified procedure set out in Chapter III.

Recommendation 37 and Special Recommendation V (Dual criminality relating to extradition)

963. The universally recognised dual criminality principle strictly applies in the extradition context. One fundamental requirement is that the offence carries an imprisonment of one year or more in India and in the foreign State (Extradition Act s.2). The Indian authorities informed the assessment team that provided the offence is punishable in India for more than a year, in practice, the penalty in the other country is not strictly applied. A substantial match of elements within the offence is required, but technical differences will not prevent extradition.

964. As already highlighted in the context of MLA (see Section 6.3 above), there is a problem resulting from the legal restrictions to the criminalisation of ML and FT when the request is subjected to the dual criminality test. ML and FT based extradition requests that do not find a counterpart offence under Indian law will then fail to meet the dual criminality requirement.

Recommendation 32 - Statistics

Statistics: Incoming Extradition requests

| | 2006 | 2007 | 2008 | up to June 2009 |
|--------------------|---------------------|---|----------------------------------|--------------------------|
| Concluded requests | Nil | 4 | 1 | Nil |
| Processed requests | 1 | 14 | 7 | 2 |
| Pending requests | 1 | 6 | 5 | 2 |
| Rejected requests | Nil | 3 One withdrawn | 1 | Nil |
| Nature of offence | Official Secret Act | Drugs, Murder, Cheating and Criminal conspiracy | Cheating and Criminal conspiracy | Criminal Breach of trust |

Statistics: Outgoing Extradition requests

| | 2006 | 2007 | 2008 | 2009 up to June, 2009 |
|--------------------|---------------------------------|----------------------------------|----------------------------------|-----------------------|
| Concluded requests | Nil | 4 | 6 | Nil |
| Processed requests | 2 | 3 | 6 | 1 |
| Pending requests | 6 | 1 | 1 | Nil |
| Rejected requests | Nil | Nil | Nil | Nil |
| Nature of offence | Man Slaughter & Financial Fraud | Drug, Murder and Financial Fraud | Drug, Murder and Financial Fraud | Murder |

965. The four rejected incoming requests for extradition were trialled in absentia for the offences. As the Indian legal system does not recognise trial in absentia (see Section 2.3 above), India does not accept an extradition request in absentia of the defendant unless an assurance is given that the accused shall be re-tried providing full opportunity to defend him.

Implementation and effectiveness

966. India has a comprehensive and basically sound extradition regime. The procedures for extradition are clear and straightforward. Both the ML and FT offences meet the minimum punishment threshold and are extraditable offences. The strict application of the dual criminality principle however negatively impacts on India's legal capacity to extradite for ML:

- foreign ML conduct that does not meet the PMLA monetary threshold does not constitute an offence in India; and
- the tight connection between the predicate and the ML offence, which marks the Indian AML approach, and the consequent restriction to the criminalisation of ML activity (see Section 2.1 for more details), will conflict with foreign requests based on ML activity predicated by offences that are not predicates in India, or – more importantly – based on stand-alone ML prosecutions or convictions where the predicate is unknown or not identified.

967. Terrorist financing and terrorist acts are also extraditable offences as such but the deficiencies in the definitions and criminalisation of FT (see Section 2.2 above) may also affect the possibility to extradite when the dual criminality test is applied.

968. India can extradite its own nationals. Where another country with which India has an extradition relationship bars the extradition of its own citizens, India may do the same. If a criminal is not extradited, he can be prosecuted in India instead.

969. It should be noted that until now, India has not received nor made extradition requests for ML or FT. According to the Indian authorities, other extradition requests have taken between six to 12 months to handle. There are however some countries who have encountered problems in this regard with India. Problems have been reported related to the delay the Indian authorities have in providing assistance on extradition, if extradition takes place at all. This raises concerns about the effectiveness of the extradition system in place in India.

6.4.2 Recommendations and Comments

970. It is recommended that, within the legal boundaries of due process, India gives high priority to providing assistance with regard to extradition in a timely manner.

971. The Indian extradition procedures in place would certainly benefit from certain changes in the legal system. Therefore, the Indian authorities should rectify domestic shortcomings regarding criminalisation which also affect the possibilities to assist other countries with extradition.

6.4.3 Compliance with Recommendations 37 and 39, and Special Recommendation V

| | Rating | Summary of factors relevant to s.6.4 underlying overall rating |
|------|--------|--|
| R.39 | LC | <ul style="list-style-type: none"> • Limitations in the criminalisation of ML may limit the possibilities for extradition (dual criminality). • Effectiveness issue: <ul style="list-style-type: none"> ◦ India does not provide extradition in a timely manner. |
| R.37 | LC | <ul style="list-style-type: none"> • Limitations in the criminalisation of ML may limit the possibilities for extradition (dual criminality). |
| SR.V | LC | <ul style="list-style-type: none"> • Deficiencies in the criminalisation of FT may affect the extradition possibilities. |

6.5 Other Forms of International Co-operation (R.40 & SR.V)

6.5.1 Description and Analysis

Recommendation 40 and Special Recommendation V

General overview

The Financial Intelligence Unit of India (FIU-IND) and the law enforcement agencies are able to provide a wide range of international co-operation to their foreign counterparts both with regard to AML and CFT. Information exchange that takes place through bilateral or multilateral arrangements is based on relevant provisions in the laws and regulations governing the functioning of these institutions. Where information is provided on the basis of reciprocity, mutually agreed conditions govern the exchange of information.

972. The Indian authorities report that the FIU-IND and the law enforcement authorities are generally able to provide co-operation to their foreign counterparts in a rapid, constructive and effective manner and that they do not refuse requests for co-operation on the sole ground that the request is also considered to involve fiscal matters. In addition, the FIU-IND and the law enforcement authorities do not refuse requests for co-operation on the grounds of secrecy laws. The information exchange is not subject to disproportionate or unduly restrictive conditions. The powers of the FIU-IND and the law enforcement agencies to obtain information and relevant documents from financial institutions can be used for the execution of requests from foreign counterparts.

973. Adequate precautions are in place to ensure confidentiality of information and data protection. As a general rule, information is provided on the condition that it shall be used only for the purpose for which it has been requested, unless the requested country agrees otherwise, and that it shall be accorded the same degree of protection as the requesting country extends to information protected under its relevant domestic legislation.

974. The financial sector supervisors are currently lacking a legal basis for the exchange of confidential information with supervisors in other countries. The information exchange between these institutions and their foreign counterparts is therefore restricted to high-level information and does not extend to customer specific information.

975. On a more general level, the Ministry of External Affairs (MEA) co-ordinates the efforts of the Government of India to combat terrorism with other nations through the mechanism of Joint Working Groups (JWGs). The JWGs provide a forum for counter-terrorism co-operation with respect to sharing of information, including the results of risk assessments, regarding global and regional terrorism; training and capacity building; and strengthening of multilateral efforts in the area of CFT and counter-terrorism in more general terms. The MEA has constituted JWGs with 27 countries and two regional groups (the European Union and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Co-operation). Various government departments and agencies (Cabinet Secretariat, Ministry of Home Affairs Intelligence Bureau, Ministry of Finance – Department of Economic Affairs and Department of Revenue,

the FIU-IND, Narcotics Control Bureau, and Central Bureau of Investigation) are represented on the JWG's.

FIU to FIU exchange of information

976. The FIU-IND has been a member of the Egmont Group since May 2007 and is exchanging information with foreign FIUs via the Egmont Secure Web. The FIU-IND provides information in response to specific requests received from foreign FIUs, but also forwards information spontaneously, if it considers that this information will be relevant to a foreign FIU. Similarly, information is received from foreign FIUs both on request and in the form of spontaneous referrals.

977. The FIU-IND has also been actively involved in various projects of the Egmont Operational Working Group to develop new platforms and mechanisms to further enhance co-operation between FIUs.

978. Pursuant to the Office Memorandum (OM) of 18 November 2004, the Government of India has empowered the FIU-IND to exchange information with foreign FIUs. One of the four core functions of the FIU-IND included in the OM is: "facilitating, administering and negotiating memoranda of understanding (MOUs) with foreign FIUs". As on December 2009, the FIU-IND has signed MOUs with counterpart FIUs in the following seven countries: Mauritius; Philippines; Brazil; Malaysia; Russia; Australia and Canada.

979. The FIU-IND has the same powers for the processing of information requests from other FIUs as for the analysis of the STRs and CTRs received. This means that the FIU can (a) search its own databases (b) search public databases and (c) obtain information upon request from other Indian competent authorities, including law enforcement agencies. In the latter cases, the FIU-IND informs the competent authority about the purpose of its request as well as on whose behalf the information is being requested. In addition, the powers of the FIU to seek additional information from the reporting entities (PMLA s.13) can also be used in relation to specific requests received from foreign counterparts. However, financial information is only shared on the basis of mutual reciprocity and confidentiality.

980. The FIU-IND accepts to send requests for information to its foreign counterparts on behalf of the domestic law enforcement agencies. In such cases, the FIU-IND informs the foreign FIU that the request is sent on behalf of an Indian law enforcement agency. The information subsequently received from the foreign FIU is forwarded to the requesting law enforcement authority in line with the Egmont Group Principles of Information Exchange.

981. The FIU-IND has put in place adequate controls and safeguards to ensure that the information exchanged is used only in an authorised manner. The controls and safeguards of the FIU-IND have been reviewed by the Outreach Working Group of the Egmont Group during its visit to India in April 2006, in view of India's membership of the Egmont Group, and were considered to be meeting the Group's standards taking into account that the FIU-IND is now a member of the Egmont Group.

982. The following table provides the number of information requests with foreign FIU's from 65 countries since the FIU became operational in March 2006:

Statistics: Exchange of information by the FIU-IND

| Exchange Type | 2006 - 2007 | 2007 - 2008 | 2008 - 2009 | 2009-2010 (Up to December 2009) | Total |
|--------------------------------|-------------|-------------|-------------|------------------------------------|------------|
| Information requests made | 2 | 13 | 17 | 34 | 66 |
| Information requests received | 14 | 39 | 69 | 66 | 188 |
| Spontaneous referrals made | 0 | 4 | 4 | 4 | 12 |
| Spontaneous referrals received | 1 | 4 | 10 | 7 | 22 |

Indian Customs

983. At the international level, the Indian Customs uses a range of co-operative arrangements with other customs administrations; both under the provisions of bilateral arrangements for assistance and as a signatory to relevant international conventions (see Section 2.7 of this report). The following table gives an overview of the international requests for information received and sent by the Indian customs authorities; however, the table does not show how many of these requests related to ML or FT.

Statistics: Exchange of information by the Indian Customs

| | 2006-2007 | 2007-2008 | 2008-2009 | 2009-2010 |
|-------------------|-----------|-----------|-----------|-----------|
| Requests received | 14 | 90 | 65 | 24 |
| Requests sent | 12 | 61 | 41 | 3 |

Police to Police exchange of information**Narcotics Control Bureau (NCB)**

984. India is a signatory to the United Nations Convention Against Illicit Trafficking In Narcotic Drugs And Psychotropic Substances, and the SAARC Convention On Narcotic Drugs And Psychotropic Substances, and according to the Indian authorities, the NCB extends a wide range of co-operation as per the provisions of these Conventions. International co-operation is also extended under the provisions of bilateral co-operation agreements, and on the basis of reciprocity.

985. The NCB has received 20, 18 and 17 requests from foreign agencies in drug related cases in 2006, 2007 and 2008 respectively. In all such cases, follow up action was undertaken and the results were conveyed to the requesting State. In 2006, 2007, 2008 and 2009, one, six, seven and one controlled delivery (CD) operations against drug traffickers were undertaken respectively in co-operation with the USA, the UK and South African authorities. In addition, a number of joint operations have been conducted against illicit internet pharmacies with the Drugs Enforcement Agency (DEA) of the USA, and five such cases have been detected and dismantled during 2006-2008. So far, laundering of drug proceeds in the CD operations and illicit internet pharmacies cases has not been reported by the DEA (USA) or any other foreign agency. However, assets and properties worth millions of dollars have been frozen/seized in other countries on the basis of coordinated operations by the NCB and foreign law enforcement agencies.

Directorate of Enforcement (ED)

986. The Directorate of Enforcement is regularly exchanging information with its counterparts in foreign jurisdictions in relation to potential money laundering cases. In the past two years, for example, information has been exchanged in four such cases with the USA and in five cases with UK.

Central Bureau of Investigation (CBI)

987. The CBI, a Central investigating agency functioning under the Central Government, is designated as the National Central Bureau of India (NCB-India). The NCB-India provides assistance in investigation of offences on the basis of a request received from other countries and is also linked through Interpol's global police communications system (I-24/7) with other NCBs. The various notices issued by the Interpol such as *Red Corner Notice* are also given due importance. The NCB-India is also provided assistance by all the State Police forces. This mechanism provides for information exchange over and above MLA channels.

NIA and State Police forces

988. The NIA and all State Police forces exchange information with their foreign counterparts through the National Central Bureau India (NCB India) which is linked through Interpol's global police communication system (I-24/7). Relevant statistics in this regard are included in the table below:

| | July to December 2006 | January to December 2007 | January to December 2008 | January to 31 st August 2009 |
|-------------------------------|-----------------------|--------------------------|--------------------------|---|
| Information requests received | 1 660 | 4 489 | 4 570 | 2 983 |
| Information requests sent | 1 591 | 3 281 | 2 403 | 1 990 |

*Supervisor to supervisor exchange of information**General*

989. None of the three main regulatory authorities (with the partial exception of the SEBI) has explicit provisions in its governing legislation that specifies the circumstances in which the agency may exchange confidential information with foreign counterparts, or the safeguards that should exist if it were to exchange such information. However, the authorities have indicated that the agencies work on the principle that they are able to take whatever measures they consider appropriate to fulfil their general objectives, unless they are explicitly prohibited by law. Therefore, all three agencies have indicated that they have developed procedures that permit confidential information to be exchanged.

Reserve Bank of India (RBI)

990. The RBI Act is entirely silent with regard to international co-operation with regulatory counterparts. While, in practice, the RBI does co-operate directly with counterparts, the information exchange concentrates on the prudential regulation, in general, and the fit and proper regime, including any misconduct related to ML and FT, in particular. Since the RBI has no legal authority to request and obtain customer-specific information for the exchange of information with its international counterparts, it is unable to share this kind of information directly. However, the authorities have stated that, in the event that information, such as details of client accounts, were requested by a foreign regulator as part of an AML/CFT investigation, the RBI would be able to refer the request to the FIU-IND; which has the authority to obtain such information from financial institutions; but no such procedures have yet been employed.

991. The following table gives an overview of the information exchange between the RBI and its counterpart banking supervisors in relation to “fit and proper” enquiries (not AML/CFT specific):

Statistics: International Co-operation by the RBI

| | Financial year 2007-2008 | Financial year 2008-2009 | April to June 2009 | July to December 2009 | Total |
|--|--------------------------|--------------------------|--|-----------------------|-------|
| Information requests received | 83 from 21 countries | 100 from 19 countries | 43 from 17 countries | 58 from 9 countries | 284 |
| Responses to information requests received | all 83 | all 100 | 39 and further information is sought for the 4 outstanding request | All 58 | 284 |
| Information requests made | 1 | 8 to 8 countries | 10 to 10 countries | 11 to 8 countries | 30 |
| Responses to information requests made | 1 | 6 | 10 | 6 | 23 |

The Securities and Exchange Board of India

992. The SEBI Act does not contain any detailed statutory gateways governing information exchange with foreign counterparts. However, section 11(2)(1a) of the SEBI Act provides for the "calling from or furnishing to any such agencies, as may be specified by the Board, such information as may be considered necessary by it for the efficient discharge of its functions". The authorities clarified that, in practice, the approval of the Board is not sought for every single request, although the Board has laid down general principles in relation to international co-operation. When required to exchange information in the normal course of business, the operational departments will simply obtain the approval of the relevant Head of Department, Executive Director, full-time Board Members or Chairman, depending on the nature of the case.

993. Notwithstanding the absence of any specific statutory gateways that specify the conditions under which co-operation may be extended, the SEBI is signatory to the IOSCO Multilateral Memorandum of Understanding (MMOU) concerning consultation and exchange of information. The MMOU contains general principles regarding mutual assistance and the exchange of information. The scope of assistance under the MMOU includes providing information and documents held in the files of the requested authority, obtaining information and documents regarding matters set forth in the request for assistance, compelling a person's statement, or where, permissible, testimony under oath, etc. There are specific conditions in the MMOU to ensure that information is used only for the authorised purpose and in the manner determined by the competent (requested) authority. In addition, SEBI has signed 17 bilateral MOUs with supervisory authorities in other jurisdictions.

Statistics: International Co-operation by the SEBI

| | 2006-2007 | 2007-2008 | 2008-2009 | Up to December 2009 | Total |
|--|-----------|-----------|-----------|---------------------|-------|
| Information requests received | 22 (2) | 10 (1) | 18 (3) | 20 (4) | 70 |
| Responses to information requests received | 22 | 10 | 16 | 15 | 63 |
| Information requests made | 1 | 1 | 1 | 14 (13) | 17 |
| Responses to information requests made | 1 | 1 | 1 | 6 | 9 |
| Bilateral MOUs signed by SEBI with overseas Regulators | 2 | 7 | 1 | 2 | 12 |

Figures in brackets refer to cases of securities markets related investigations/enquiries.

The Insurance Regulatory and Development Authority (IRDA)

994. There are no specific statutory gateways for international co-operation by IRDA, and IRDA has no legal basis to exchange customer-specific information. Indian authorities informed the assessment team that IRDA has responded to six requests from foreign counterparts from Singapore and Tanzania between 2008 and March 2010.

6.5.2 Recommendations and Comments

995. The Indian authorities should ensure that:

- There are clear and effective gateways and mechanisms in place that will facilitate and allow for prompt and constructive formal exchanges of information between the supervisory authorities and their counterparts, including customer specific information.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

| | Rating | Summary of factors relevant to s.6.5 underlying overall rating |
|-------------|-----------|--|
| R.40 | LC | <ul style="list-style-type: none"> • There are no clear and effective gateways and mechanisms in place for the RBI and IRDA that allow for prompt and constructive exchanges of confidential information with foreign counterparts. |
| SR.V | LC | <ul style="list-style-type: none"> • There are no clear and effective gateways and mechanisms in place for the RBI and IRDA that allow for prompt and constructive exchanges of confidential information with foreign counterparts. |

7. OTHER ISSUES

7.1 *Resources and statistics*

| | Rating | Summary of factors relevant to Recommendations 30 and 32 underlying overall rating |
|-------------|-----------|---|
| R.30 | LC | <ul style="list-style-type: none"> Concerns about the adequacy of staffing levels in the IRDA. Uncertainties about the future regulatory regime for the banking activities of India Post. |
| R.32 | LC | <ul style="list-style-type: none"> No statistics available regarding the number of CDFs collected at Land Customs Stations and detections of smuggling of currency and BNI through the mail and containerised cargo. |

7.2 *Other Relevant AML/CFT Measures or Issues*

996. There are no further issues to be discussed in this section.

7.3 *General framework for AML/CFT system (see also section 1.1)*

997. There are no further issues to be discussed in this section.

TABLES

Table 1: Ratings of Compliance with FATF Recommendations

Table 2: Recommended Action Plan to improve the AML/CFT system

Table 3: Authorities' Response to the Evaluation (if necessary)

Table 1: Ratings of Compliance with FATF Recommendations

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (na).

| Forty Recommendations | Rating | Summary of factors underlying rating ⁷⁶ |
|--|--------|--|
| Legal system | | |
| 1. ML offence | PC | <ul style="list-style-type: none"> • (High) monetary threshold condition for most ML predicates. • ML provision does not cover physical concealment of criminal proceeds. • ML provision does not cover the sole knowing acquisition, possession and use of criminal proceeds. • Effectiveness issues: <ul style="list-style-type: none"> ○ the absence of any conviction for ML; ○ the high evidentiary standard untested before the courts, particularly in respect of the proof of the foreign predicate offence. |
| 2. ML offence – mental element and corporate liability | LC | <ul style="list-style-type: none"> • Inadequate sanctions for legal persons committing the ML offence. • Effectiveness issues: <ul style="list-style-type: none"> ○ the total absence of ML convictions; ○ the interpretation of making corporate criminal liability contingent on prosecution of a natural person. |
| 3. Confiscation and provisional measures | PC | <ul style="list-style-type: none"> • Confiscation of property laundered is not covered in the relevant legislation and depends on a conviction for a scheduled predicate offence. • The UAPA does not allow for confiscation of intended instrumentalities used in terrorist acts or funds collected to be used by terrorist individuals. • The UAPA and NDPS Act do not allow for property of corresponding value to be confiscated. • There are no clear provisions and procedures on how to deal with the assets in case of criminal proceedings when the defendant has died. • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns based on the limited number of confiscations in relation to ML/FT offences. |
| Preventive measures | | |
| 4. Secrecy laws consistent with the Recommendations | C | This Recommendation is fully observed. |
| 5. Customer due diligence | PC | <ul style="list-style-type: none"> • Scope limitation: |

⁷⁶

These factors are only required to be set out when the rating is less than Compliant.

| Forty Recommendations | Rating | Summary of factors underlying rating ⁷⁶ |
|---|--------|--|
| | | <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • No provisions in law or regulation that require CDD to be renewed when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data. • No provisions in law or regulation that require an institution proactively to determine whether a customer is acting on behalf of another person. • Lack of clarity and divergent practices in relation to the identification and verification of beneficial ownership. • Professional secrecy provisions prevent identification of beneficial owners of client accounts. • No obligation in IRDA circular to understand ownership and control structures of legal persons. • The RBI and IRDA circulars do not require a specific override of the procedures for low risk customers when there are suspicions of ML/FT, or where factors suggest that the customer poses a higher risk. • No explicit requirement in the RBI and IRDA circulars to consider filing an STR when the institution can no longer be satisfied that it knows the true identity of the customer. • Term life policies exempt from AML requirements at stage of writing the policy. • Implementation issue: <ul style="list-style-type: none"> ○ recent introduction of the Authorised Persons within the PMLA (including India Post) results in questions over extent of implementation. |
| 6. Politically exposed persons | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • No requirement in the RBI and SEBI circulars to implement ongoing risk management procedures for identifying PEPs. • No requirement in the RBI circulars to apply enhanced measures to close relatives of PEPs. • No obligation in the IRDA circular to apply enhanced measures to entities where the beneficial owner of the customer is a PEP. |
| 7. Correspondent banking | LC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ no evidence provided that implementation is effective. |
| 8. New technologies & non face-to-face business | LC | <ul style="list-style-type: none"> • Inadequate provisions in the IRDA circulars to address the issues of technological developments and non-face-to-face business. |
| 9. Third parties and introducers | N/A | This Recommendation is not applicable in India. |
| 10. Record keeping | LC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • The requirement that customer identification records need to be maintained for at least five years from the termination of the account or business relationship is not contained in law or regulation. • Sector specific circulars have exempted some insurance products, including term life policies, from AML requirements. |
| 11. Unusual transactions | LC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • Effectiveness issue: <ul style="list-style-type: none"> ○ Authorised Persons and Payments Service Operators, including India Post, are only covered by the PMLA as of June 2009, making it too soon to assess effectiveness. |
| 12. DNFBP – R.5, 6, 8-11 | NC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to any of the DNFBP sectors, with the exception of casinos. • Only the basic requirements of the PMLA and the accompanying Rules apply to casinos, and these do not address much of the detail required under the FATF standards. |

| Forty Recommendations | Rating | Summary of factors underlying rating ⁷⁶ |
|---|--------|---|
| | | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ extension of the PMLA to the casino sector is very recent and there is insufficient evidence of effective implementation. |
| 13. Suspicious transaction reporting | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. ○ There is no definition of “activities of terrorism” in the PMLA, leaving it to reporting institutions to interpret the scope of the STR reporting requirement with respect to the financing of the activities of terrorism. • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns about the low number of STRs filed in relation to ML and FT (especially in relation to the banking sector). |
| 14. Protection & no tipping-off | LC | <ul style="list-style-type: none"> • Directors or employees are not expressly covered by the PMLA’s safe harbour provision. |
| 15. Internal controls, compliance & audit | LC | <ul style="list-style-type: none"> • The role of the principal officer in the banking sector (except for AMCs) is defined in terms simply of STR and other reporting, and does not extend to overall compliance. • There is no express requirement that the audit function in the securities sector should be adequately resourced, and the resource issue is not expressly addressed in insurance sector. |
| 16. DNFBP – R.13-15 & 21 | NC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to any of the DNFBP sectors, with the exception of casinos. • Only the basic requirements of the PMLA and the accompanying rules apply to casinos, and these do not address much of the detail required under the FATF standards. • Implementation issue: <ul style="list-style-type: none"> ○ extension of the PMLA to the casino sector is very recent and there is insufficient evidence of effective implementation. |
| 17. Sanctions | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • Sanctions applied for AML/CFT deficiencies across all sectors are not effective, proportionate or dissuasive. |
| 18. Shell banks | LC | <ul style="list-style-type: none"> • There is no guidance for financial institutions regarding measures that should be in place to satisfy themselves that they are not entering into relationships with shell banks or that their foreign respondent institutions do not permit their accounts to be used by shell banks. |
| 19. Other forms of reporting | C | This Recommendation is fully observed. |
| 20. Other NFBP & secure transaction techniques | LC | <ul style="list-style-type: none"> • No consideration given to extending the AML/CFT provisions to other than DNFBPs. |
| 21. Special attention for higher risk countries | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • There are no clear and direct requirements for the institutions in the banking and insurance sectors to pay special attention to both business relationships and transactions with persons from or in countries that do not, or insufficiently, apply the FATF Recommendations. • Financial institutions are not expressly required to examine the background and purpose of transactions with persons from or in countries that do not adequately apply the FATF standards. • India has no clear legal authority that enables it to apply a range of appropriate counter-measures in the securities or insurance sectors where a country continues not to apply or insufficiently applies the FATF Recommendations. • Effectiveness issue: <ul style="list-style-type: none"> ○ there is a concern that covered institutions do not look beyond the FATF statements, and that they make little use of publicly available information when identifying countries which do not or insufficiently apply the FATF |

| Forty Recommendations | Rating | Summary of factors underlying rating ⁷⁶ |
|--|--------|--|
| | | Recommendations. |
| 22. Foreign branches & subsidiaries | C | <ul style="list-style-type: none"> This Recommendation is fully observed. |
| 23. Regulation, supervision and monitoring | PC | <ul style="list-style-type: none"> Scope limitation: <ul style="list-style-type: none"> the PMLA does not apply to commodities futures brokers. Fit and proper testing by regulators prior to appointment does not apply to Non-executive Directors. Effectiveness issues: <ul style="list-style-type: none"> Authorised Persons and Payment Service Providers, including India Post, have only recently been brought under the PMLA, and hence it is too early to assess effectiveness; no inspections or ongoing monitoring by the Ministry of Finance of India Post as yet; concerns that the regulators' procedures for targeting on-site inspections do not adequately take into account the AML/CFT risks of individual institutions. |
| 24. DNFBP - regulation, supervision and monitoring | NC | <ul style="list-style-type: none"> Scope limitation: <ul style="list-style-type: none"> the PMLA does not apply to any of the DNFBP sectors, with the exception of casinos. With respect to the casino sector: <ul style="list-style-type: none"> No statutory "fit and proper" tests for owners, operators and managers. Insufficient range of sanctions available to the regulator to permit a proportionate response to identified deficiencies. Doubts about the statutory authority of the regulator to enforce compliance with the PML Rules and its own AML/CFT circular. Lack of dissuasive sanctions for obstructing the regulator's right to inspect. |
| 25. Guidelines & Feedback | LC | <ul style="list-style-type: none"> Written guidance provided to the casino sector to assist with the implementation of the PML rules is limited in scope. |
| Institutional and other measures | | |
| 26. The FIU | LC | <ul style="list-style-type: none"> Effectiveness issue: <ul style="list-style-type: none"> the dissemination of financial information for investigation or action by the State Police is relatively low in comparison with the State Police's primary responsibility for the investigation and prosecution of FT and predicate offences to money laundering, and for confiscation of proceeds of crime. Public information released by the FIU-IND does not include information on typologies and trends in ML and FT cases and related predicate offences. |
| 27. Law enforcement authorities | LC | <ul style="list-style-type: none"> Effectiveness issue: <ul style="list-style-type: none"> India has yet to achieve ML convictions. |
| 28. Powers of competent authorities | C | This Recommendation is fully observed. |
| 29. Supervisors | LC | <ul style="list-style-type: none"> Scope limitation: <ul style="list-style-type: none"> the PMLA does not apply to commodities futures brokers. Financial sanctions applied for AML/CFT deficiencies across all sectors are not effective, proportionate or dissuasive. There is no established supervisory regime covering the banking operations of India Post. |
| 30. Resources, integrity and training | LC | <ul style="list-style-type: none"> Concerns about the adequacy of staffing levels in the IRDA. Uncertainties about the future regulatory regime for the banking activities of India Post. |
| 31. National co-operation | LC | <ul style="list-style-type: none"> Effectiveness issue: <ul style="list-style-type: none"> the effectiveness of the inter-agency co-ordination and co-operation has not yet been demonstrated. |

| Forty Recommendations | Rating | Summary of factors underlying rating⁷⁶ |
|--|---------------|--|
| 32. Statistics | LC | <ul style="list-style-type: none"> No statistics available regarding the number of CDFs collected at Land Customs Stations and detections of smuggling of currency and BNI through the mail and containerised cargo. |
| 33. Legal persons – beneficial owners | PC | <ul style="list-style-type: none"> Information on additional beneficial ownership of legal persons beyond the immediate beneficial owner is not required to be collected by either the corporate registry, within corporate records held by legal persons, or by company secretaries. There are no measures in place to prevent the unlawful use of HUFs in relation to ML or FT – for instance, HUFs are not required to maintain information on beneficial ownership. While law enforcement and other authorities have sufficient powers to access current and accurate information on beneficial ownership of legal persons (in particular foreign companies), this is not possible in a timely fashion. |
| 34. Legal arrangements – beneficial owners | PC | <ul style="list-style-type: none"> There is no requirement to obtain, verify and retain adequate, accurate and current information on the beneficial ownership and control of private trusts. That are no measures in place that guarantee that minimal adequate and accurate information concerning the beneficial owners of private trusts can be obtained or accessed by the competent authorities in a timely fashion. |
| International Co-operation | | |
| 35. Conventions | PC | <ul style="list-style-type: none"> Palermo TOC Convention not ratified. Criminalisation of ML not in line with the Vienna and TOC Conventions (concealment, acquisition, possession and use). Restricted ML seizure/confiscation regime. Inadequate sanctions for the ML offence in the NDPS Act and the sanctions for legal persons in the PMLA. Deficiencies in the regulatory and supervisory regime. Effectiveness issue: <ul style="list-style-type: none"> absence of convictions. |
| 36. Mutual legal assistance (MLA) | LC | <ul style="list-style-type: none"> MLA in coercive actions may be hampered as a result of domestic legal deficiencies (dual criminality). Effectiveness issue: <ul style="list-style-type: none"> India does not provide MLA in a timely manner. |
| 37. Dual criminality | LC | <ul style="list-style-type: none"> MLA in coercive actions may be hampered as a result of domestic legal deficiencies (dual criminality). Limitations in the criminalisation of ML may limit the possibilities for extradition (dual criminality). |
| 38. MLA on confiscation and freezing | LC | <ul style="list-style-type: none"> Deficiencies in confiscation regime of laundered property, instrumentalities and proceeds of money laundering affect the MLA capability. |
| 39. Extradition | LC | <ul style="list-style-type: none"> Limitations in the criminalisation of ML may limit the possibilities for extradition (dual criminality). Effectiveness issue: <ul style="list-style-type: none"> India does not provide extradition in a timely manner. |
| 40. Other forms of co-operation | LC | <ul style="list-style-type: none"> There are no clear and effective gateways and mechanisms in place for the RBI and IRDA that allow for prompt and constructive exchanges of confidential information with foreign counterparts. |

| Nine Special Recommendations | Rating | Summary of factors underlying rating |
|-------------------------------------|---------------|--|
| SR.I Implement UN instruments | PC | <ul style="list-style-type: none"> FT criminalisation not in line with the FT Convention (FT offences, international organisations, attempt). Confiscation of terrorist funds is deficient. UN RES are not fully implemented. Effectiveness issue: <ul style="list-style-type: none"> concerns regarding preventive regime and judicial follow-up in terms of final convictions. |

| Nine Special Recommendations | Rating | Summary of factors underlying rating |
|--|--------|---|
| SR.II Criminalise terrorist financing | PC | <ul style="list-style-type: none"> • FT provisions not in line with the FT Convention: <ul style="list-style-type: none"> ○ criminalisation of Treaty offences not consistent with art. 2.1(a); ○ not all Treaty offences included in the list of terrorist acts; ○ international organisations not covered; ○ FT attempt is not fully covered. • No criminalisation of sole knowing funding of terrorist individuals and terrorist organisations. • Effectiveness issue: <ul style="list-style-type: none"> ○ minimal number of convictions. |
| SR.III Freeze and confiscate terrorist assets | LC | <ul style="list-style-type: none"> • There is no indication of effective implementation of the guidelines recently issued for the DNFBP sector. • There is no monitoring mechanism in place to ensure compliance with the freezing mechanism outside the financial sector. • There are no procedures in place that allow affected persons to have access to funds for basic expenses. |
| SR.IV Suspicious transaction reporting | PC | <ul style="list-style-type: none"> • Scope limitation: <ul style="list-style-type: none"> ○ the PMLA does not apply to commodities futures brokers. • There is no definition of “activities of terrorism” in the PMLA, leaving it to reporting institutions to interpret the scope of the STR reporting requirement with respect to the financing of the activities of terrorism. • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns about the extremely low number of STRs filed in relation to FT in comparison with India’s vulnerability with regard to terrorism |
| SR.V International co-operation | LC | <ul style="list-style-type: none"> • MLA in coercive actions may be hampered as a result of domestic legal deficiencies (dual criminality). • Deficiencies in the confiscation regime related to FT affect the MLA capability. • Deficiencies in the criminalisation of FT may affect the extradition possibilities. • There are no clear and effective gateways and mechanisms in place for the RBI and IRDA that allow for prompt and constructive exchanges of confidential information with foreign counterparts. |
| SR.VI AML requirements for money/value transfer services | LC | <ul style="list-style-type: none"> • The application of the FATF Recommendations to MVTS providers suffers from the same deficiencies as identified in relation to the rest of the financial sector (see sections 3.1 to 3.10 of this report). |
| SR. VII Wire transfer rules | LC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ the PMLA did not apply to India Post, which is authorised to conduct both domestic and cross border wire transfers, until June 2009. |
| SR.VIII Non-profit organisations | NC | <ul style="list-style-type: none"> • There is no review undertaken of the adequacy of domestic laws in the NPO sector. • There are no periodic reassessments undertaken by reviewing new information on the sector’s potential vulnerabilities to terrorist activities. • There is no outreach to the NPO sector with a view to protecting the sector from abuse for terrorist financing takes place. • There is only limited information available on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. • India has not demonstrated that measures are in place to sanction violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs for NPOs other than those registered under the Income Tax Act and under the FCRA. • The majority of NPOs are not registered as such with government agencies, including the tax authorities. |

| Nine Special Recommendations | Rating | Summary of factors underlying rating |
|---|--------|---|
| SR.IX Cross Border Declaration & Disclosure | PC | <ul style="list-style-type: none"> • Effectiveness issue: <ul style="list-style-type: none"> ○ concerns based on the low number of currency declarations, the detected false declarations, and the cash seizures, including seizures of unaccompanied cash or BNIs. • The Cross border declaration/disclosure systems appear to be applied only to currency and BNI via airports, with no information on movements of currency and BNI via land borders or unaccompanied movement of currency through postal and cargo systems. • The shortcomings identified with regard to the attachment, confiscation and forfeiture provisions discussed in Section 2.3 and to the freezing, seizing and attachment of property related to terrorist financing (as discussed in Section 2.4) have a negative impact on Special Recommendation IX. |

Table 2: Recommended Action Plan to Improve the AML/CFT System

| AML/CFT system | Recommended Action |
|---|---|
| 1. General | No text required |
| 2. Legal System and Related Institutional | |
| 2.1 Criminalisation of Money laundering Measures (R.1 & R.2) | <p>Although recently an increased focus on the ML aspect and use of the ML provisions is to be acknowledged, there are still some important and often long-standing legal issues to be resolved. To that end following measures should be taken:</p> <ul style="list-style-type: none"> • The monetary threshold limitation of INR 3 million for the Schedule Part B predicate offences should be abolished. • The section 3 PMLA definition of the ML offence should be brought in line with the Vienna and Palermo Conventions so as to also fully cover the physical concealment and the sole acquisition, possession and use of all relevant proceeds of crime. • The present strict and formalistic interpretation of the evidentiary requirements in respect of the proof of the predicate offence should be put to the test of the courts to develop case law and receive direction on this fundamental legal issue. • The level of the maximum fine imposable on legal persons should be raised or left at the discretion of the court to ensure a more dissuasive effect. • The practice of making a conviction of legal persons contingent on the concurrent prosecution/conviction of a (responsible) natural person should be abandoned. |
| 2.2 Criminalisation of Terrorist Financing (SR.II) | <p>There are a number of deficiencies that need to be addressed to bring the offence more in line with the relevant international standards and, by doing so, enhance the effectiveness of the CFT system itself.</p> <ul style="list-style-type: none"> • The <u>sole</u> (intentional or knowing) financing of the offences covered by the Treaties annexed to the FT Convention should be criminalised as terrorist financing • The section 16A UAPA offence of making demands for nuclear material, etc. should be included in the section 15 list of terrorist acts. • The terrorist acts under section 15 of the UAPA should also target international organisations. • The attempt to commit the section 17 and section 40 UAPA offences should be fully covered. • The sole wilful financing of terrorist individuals and terrorist organisations should be criminalised. |
| 2.3 Confiscation, freezing and seizing of proceeds of crime (R.3) | <p>Although the confiscation regime in India allows for a broad spectrum of seizure and forfeiture measures in the AML/CFT context, it is not fully comprehensive and does show a number of (legal) deficiencies. Therefore it is recommended that:</p> <ul style="list-style-type: none"> • Legal measures are taken to allow for confiscation of the money laundered as subject of the ML offence and which is not contingent on a conviction for the predicate offence (stand-alone ML offence). • The Indian authorities ensure that the definition of proceeds of terrorism is wide enough to allow for confiscation of instrumentalities and funds used to finance an individual terrorist. • The UAPA and the NDPS Act should explicitly provide for full equivalent value confiscation. • The confiscation regime should also include clear provisions and procedures on how to deal with the assets in case the criminal proceedings come to a halt because of the death of the defendant. |
| 2.4 Freezing of funds used for terrorist financing (SR.III) | <p>Even though since 2007, India has introduced legislation and procedures that enable it to freeze terrorist funds, there still remain some shortcomings. It is therefore recommended that the Indian authorities ensure that:</p> <ul style="list-style-type: none"> • The guidelines recently issued for the DNFBP sector regarding the |

| AML/CFT system | Recommended Action |
|---|--|
| | <p>freezing mechanism are effectively implemented.</p> <ul style="list-style-type: none"> • A monitoring mechanism is set up to ensure compliance with the freezing mechanism outside the financial sector. • Procedures are put in place for authorising access to funds for basic expenses. |
| 2.5 The Financial Intelligence unit and its functions (R.26) | <p>It is recommended that the FIU-IND:</p> <ul style="list-style-type: none"> • Should enhance its capability in relation to intelligence and information dissemination to all competent authorities, including the State Police. • Should enhance its dissemination of public information regarding trends and typologies, which could include strategic reporting. |
| 2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28) | <ul style="list-style-type: none"> • While India has initiated a large number of ML investigations, it has yet to achieve convictions for ML offences. |
| 2.7 Cross Border Declaration & Disclosure | <p>In addition to technical deficiencies in relation to which India should consider amending its legislation, there are issues regarding the effectiveness of the implementation of both the declaration scheme for importing and the disclosure regime for export of currency and BNI's. Therefore, Indian authorities should:</p> <ul style="list-style-type: none"> • Undertake an in-depth analysis and envisage taking the necessary actions based on the deficiencies identified in relation to the arrival card for passengers used at international airports, including the absence of the necessary guidance, and the use of Customs Declaration Forms at land borders. • Introduce targeted actions for the detection of smuggling of currency and BNI via the mail and containerised cargo. • Take action to address the deficiencies identified in relation to the implementation of the FATF Recommendations, as identified in Sections 2.3 and 2.4 of this report that have a negative impact on Special Recommendation IX. |
| 3. Preventive measures – Financial institutions | |
| 3.1 Risk of money laundering or terrorist financing | <ul style="list-style-type: none"> • The authorities should undertake a comprehensive risk assessment of all the financial institutions operating in India. |
| 3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8) | <p>It is recommended that the authorities:</p> <ul style="list-style-type: none"> • Bring the commodities futures brokers fully within the scope of the PMLA. • Amend the PML Rules to: <ul style="list-style-type: none"> ○ require renewal of CDD when there are suspicions of money laundering or terrorist financing, or where there are doubts about the adequacy or veracity of previously obtained customer identification data; and ○ require institutions proactively to determine whether a customer is acting on behalf of another person. • Amend the regulatory circulars to: <ul style="list-style-type: none"> ○ implement a requirement that the low risk provisions should not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not, in fact, pose a low risk (RBI and IRDA); ○ provide guidance on how to interpret the definition of beneficial ownership and on the procedures required to identify the ultimate natural person who owns or controls the customer (all regulators); ○ introduce measures to prevent the opening of client accounts unless the professional intermediary is willing and able to provide information on the beneficial owners (RBI); ○ introduce requirement to understand the ownership and control structure of legal persons (IRDA); ○ introduce a requirement that an institution should consider filing an STR when an institution can no longer be satisfied that it knows the true identity of a customer (RBI and IRDA); and ○ remove the exemption for term life policies from the AML obligations at the time that the policy is first written (IRDA); |

| AML/CFT system | Recommended Action |
|--|--|
| | <ul style="list-style-type: none"> ○ introduce consistent requirements within all three sets of circulars to ensure that all institutions should have appropriate ongoing risk management procedures for identifying (and applying enhanced CDD to) PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner. ● Review the procedures under which the insurers are entirely reliant on the basic identification procedures carried out by their agents (IRDA). |
| 3.3 Third parties and introduced business (R.9) | <ul style="list-style-type: none"> ● In view of the potential confusion that might be caused by section 2.5(iii) of the RBI Master Circular, it is recommended that this section be amended to remove all doubt about the scope for institutions to accept business introduced by third parties, as envisaged under Recommendation 9. |
| 3.4 Financial institution secrecy or confidentiality (R.4) | <ul style="list-style-type: none"> ● There are no recommendations in relation to Recommendation 4. |
| 3.5 Record keeping and wire transfer rules (R.10 & SR.VII) | <p>It is recommended that the Indian authorities:</p> <ul style="list-style-type: none"> ● Bring the commodities futures brokers fully within the scope of the PMLA. ● Amend the PML Rules to require that: <ul style="list-style-type: none"> ○ the retention period for customer identification records extends at least five years from the termination of the account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority). ● Amend the regulatory circulars to remove the total exemption for term life policies from the AML obligations by requiring the maintenance of records of payout transactions (IRDA), including identification of beneficiaries. |
| 3.6 Monitoring of transactions and relationship (R.11 & 21) | <p>It is recommended that the Indian authorities:</p> <ul style="list-style-type: none"> ● Bring the commodities futures brokers fully within the scope of the PMLA. ● Establish clear and direct requirements for the institutions in the banking and insurance sector to pay special attention to both business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations. ● Require all financial institutions to examine the purpose of transactions with persons from or in countries that do not adequately apply the FATF standards in order to determine whether there is an apparent economic or visible lawful purpose. ● Develop adequate legal authorities to enable it to apply a range of appropriate counter-measures across all financial sectors where a country continues not to apply or insufficiently applies the FATF Recommendations. ● In order to improve the effectiveness of the measures in place, make clear that covered institutions should go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations. |
| 3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV) | <p>It is recommended that the Indian authorities:</p> <ul style="list-style-type: none"> ● Bring the commodities futures brokers fully within the scope of the PMLA. ● Thoroughly examine the STR reporting rate, to determine whether it is adequate, given the size of the financial sector and the number of proceeds-generating crimes; whether specific sectors or geographic regions are not reporting appropriate numbers of STRs; and, if STR reporting levels are inadequate, either overall or by specific sector/area of the country, the reasons for such low reporting and appropriate responses to correct the underlying problems. Particular attention should be paid to the banking sector. ● Thoroughly examine the STR reporting rate with respect to terrorism-financing related STRs in particular, to determine why the number of such STRs appears to be extremely low, both in terms of the size of the financial system and relative to the terrorist financing risk, and why so few of the FT-related STRs have been identified by means other than automated alerts triggered by matching names to terrorist lists, and take appropriate steps to correct any underlying problems. ● Conduct intensive outreach, focusing on MSBs and banks, to improve |

| AML/CFT system | Recommended Action |
|--|---|
| | <p>capacity to identify and report FT-related suspicious transactions.</p> <ul style="list-style-type: none"> Clarify the scope of the language of the STR reporting requirement covering transactions relating to the financing of the activities of terrorism to ensure that it requires covered institutions to report suspicious transactions where they suspect or there is reasonable grounds to suspect that the funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations, Expand the PMLA's safe harbour provision to expressly cover directors or employees. |
| 3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22) | <p>It is recommended that the Indian authorities:</p> <ul style="list-style-type: none"> Extend the responsibilities of the Principal Officer in the banking sector beyond the STR and other reporting to overall compliance. Expressly provide that the audit function in all sectors should be independent and adequately resourced. |
| 3.9 Shell banks (R.18) | <ul style="list-style-type: none"> It is recommended that the RBI provides guidance to financial institutions regarding measures that should be in place in order for financial institutions to satisfy themselves that they are not entering into relationships with shell banks or that their foreign respondent institutions do not permit their accounts to be used by shell banks. |
| 3.10 The supervisory and oversight system – competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25) | <ul style="list-style-type: none"> The commodities futures brokers should be brought fully within the scope of the PMLA A review should be undertaken of both the levels of financial sanctions for non-compliance with the AML/CFT requirements, and the procedures under which penalties are applied to ensure that they focus on systemic rather than transactional failings in institutions. The “fit and proper” tests prior to appointment should be extended to non-executive directors. The Ministry of Finance should develop and implement procedures for inspection and ongoing monitoring of India Post. Reviews should be undertaken by all the regulators to ensure that their procedures for targeting on-site inspections take adequate account of the AML/CFT risks of individual institutions. A review should be undertaken of the AML/CFT inspection procedures adopted by the NABARD and the NHB to ensure that they are in line with those adopted by the RBI itself. |
| 3.11 Money value transfer services (SR.VI) | <ul style="list-style-type: none"> India should take action to address the deficiencies identified in relation to the implementation of the FATF Recommendations, as identified in sections 3.1 to 3.10 of this report, in relation to MVTs providers. |
| 4. Preventive measures – Non-Financial Business and Professions | |
| 4.1 Customer due diligence and record-keeping (R.12) | <ul style="list-style-type: none"> It is clearly very early days in the extension of the AML/CFT obligations to the DNFBP sectors. While the PMLA and the accompanying Rules have been applied to the casino sector, there have been no substantive additional provisions imposed by the regulators in Goa. Therefore, it is essential that the Home Department of the Government of Goa should undertake a thorough study of the FATF standards and determine what additional instruction needs to be applied to the casinos in order to address the perceived risks and to comply with the standards. In this respect, it will clearly be helpful to review the circulars issued by the financial sector regulators and draw from their experience. As regards the other DNFBP sectors, it is important that the Government extend the PMLA to the businesses and professions as soon as possible. While the FATF standard does not envisage the complete exclusion (on a risk basis) of any of the DNFBPs from meeting the AML/CFT obligations, since they are all perceived to present a material risk, it is clearly appropriate to consider, on a risk-sensitive basis, the extent to which the range of requirements need to be applied. |

| AML/CFT system | Recommended Action |
|--|--|
| 4.2 Suspicious transaction reporting (R.16) | <ul style="list-style-type: none"> • The authorities in Goa should review the need to issue further enforceable guidance to the casino sector, especially in relation to the implementation of appropriate internal systems and controls. This is especially important in the context of the offshore casinos, which pose the greater (albeit still quite low) risk. • More generally, appropriate obligations will need to be introduced for the other DNFBP sectors once they are brought under the PMLA. |
| 4.3 Regulation, supervision and monitoring (R.24-25) | <ul style="list-style-type: none"> • It is recommended that the regulatory framework for the casino sector be extended in order to: <ul style="list-style-type: none"> ○ give the authorities statutory powers to apply “fit and proper” tests to the owners, operators and managers of casinos; ○ give the regulator the statutory authority to use its powers of inspection, etc., in order to enforce compliance with the provisions of the PMLA; ○ increase the penalty for obstructing access by the regulator, in order to make it effective and dissuasive; ○ make specific provision for sanctions to be applied for breaches of the PMLA, the accompanying Rules and any relevant instructions that the regulator may issue from time to time; and ○ broaden the scope of the sanctions that may be applied, so that there is a range of options that might be applied effectively. • The scope of the written guidance provided to the casino sector to assist with the implementation of the PML Rules needs to be extended. |
| 4.4 Other non-financial businesses and professions (R.20) | <ul style="list-style-type: none"> • India should consider extending the AML/CFT provisions to non-financial businesses and professions (other than DNFBPs). |
| 5. Legal Persons and Arrangements & Non-profit Organisations | |
| 5.1 Legal Persons – Access to beneficial ownership and control information (R.33) | <ul style="list-style-type: none"> • India should ensure that information on beneficial ownership of legal persons is collected by either the corporate registry, within corporate records held by legal persons, or by company secretaries. India should also prohibit nominee directors and nominee shareholders, or (alternatively) establish measures to mitigate the risk of ML and FT associated with those kinds of directors and shareholders. • There should be measures in place to ensure that beneficial ownership information relating to Hindu Undivided Family (HUF) businesses is available through a requirement for HUFs to register with a central registry and maintain beneficial ownership information or through other measures such as a requirement for all HUFs to obtain PANs and to maintain information on all beneficial ownership information available to law enforcement or other authorities on request. • India should take measures to ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis. The current powers of the competent authorities are hampered to the extent that the repositories of information from which the authorities could obtain information do not maintain sufficient beneficial ownership information. |
| 5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34) | <ul style="list-style-type: none"> • India should further develop requirements to ensure that information on the beneficial ownership and control of private trusts is collected and readily available to the competent authorities in a timely manner. Such measures could include, for example, requiring trustees to maintain full information on the trust’s beneficial ownership and control, requiring the location of such information to be disclosed, or requiring trust service providers to obtain and maintain beneficial ownership information. Such information would then be available to the law enforcement and other competent agencies upon the proper exercise of their existing powers. |
| 5.3 Non-profit organisations (SR.VIII) | <p>It is recommended that India should:</p> <ul style="list-style-type: none"> • Undertake a comprehensive NPO sector review capturing all relevant data necessary, including the adequacy of domestic laws in the NPO sector. • Undertake a detailed risk assessment of the sector for terrorist financing. |

| AML/CFT system | Recommended Action |
|--|--|
| | <ul style="list-style-type: none"> • Undertake comprehensive outreach to the NPO sector with a view to protecting the sector from abuse for terrorist financing as well as wider outreach in relation to good governance and accountability. • Ensure that NPOs maintain information on the identity of the persons who own, control or direct their activities, including senior officers, board members and trustees. • Demonstrate that appropriate measures are in place to sanction violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs, other than those registered under the Income Tax Act and the FCRA. • Implement measures to ensure that all NPOs are licensed and/or registered as such and make this new information available to the competent authorities. |
| 6. National and International Co-operation | |
| 6.1 National co-operation and coordination (R.31) | <ul style="list-style-type: none"> • While India has initiated a large number of ML investigations (798 at 31 December 2009), only six prosecutions are underway and there are no convictions so far. India has yet to achieve convictions and additional prosecutions that demonstrate the effectiveness of its inter-agency co-ordination and co-operation. |
| 6.2 The Conventions and UN special Resolutions (R.35 & SR.I) | <ul style="list-style-type: none"> • Besides ratifying the Palermo Convention⁷⁷, India should review its ML and FT provisions to bring them in line with the relevant Conventions, particularly in respect of the criminalisation and the implementation of the preventive regime. |
| 6.3 Mutual Legal Assistance (R.36-38 & SR.V) | <ul style="list-style-type: none"> • Although there are measures in place in the laws to provide mutual legal assistance in criminal matters and structured mechanisms for handling such requests, some shortcomings still exist. First of all, it is recommended that India gives high priority to providing MLA in a timely manner. Secondly, by addressing the identified legal deficiencies, the capacity for India for MLA would automatically be enhanced. The Indian authorities should therefore rectify domestic shortcomings regarding criminalisation, confiscation and provisional measures, which also affect the possibilities to provide MLA in coercive actions. |
| 6.4 Extradition (R.39, 37 & SR.V) | <ul style="list-style-type: none"> • It is recommended that, within the legal boundaries of due process, India gives high priority to providing assistance with regard to extradition in a timely manner. • The Indian extradition procedures in place would certainly benefit from certain changes in the legal system. Therefore, the Indian authorities should rectify domestic shortcomings regarding criminalisation which also affect the possibilities to assist other countries with extradition. |
| 6.5 Other forms of co-operation (R.40 & SR.V) | <p>The Indian authorities should ensure that:</p> <ul style="list-style-type: none"> • There are clear and effective gateways and mechanisms in place that will facilitate and allow for prompt and constructive formal exchanges of information between the supervisory authorities and their counterparts, including customer specific information. |
| Other issues | |
| 7.1 Resources and statistics (R.30 & 32) | <ul style="list-style-type: none"> • A review should be undertaken of the human resourcing of the IRDA. • India should ensure to take necessary actions to establish and effectively implement a supervisory regime for the banking activities of India Post. • India should ensure that it keeps statistics regarding the number of CDFs collected at Land Customs Stations and detections of smuggling of currency and BNI through mail and containerised cargo. |
| 7.2 Other relevant AML/CFT measures or issues | <ul style="list-style-type: none"> • There are no recommendations for this Section. |
| 7.3 General framework – structural issues | <ul style="list-style-type: none"> • There are no recommendations for this Section. |

77

The Union Cabinet of India in its meeting held on the 19 March 2010 has approved the ratification of the Palermo Convention. India is in the process to complete the necessary formalities.

