# Anti-money laundering and counter-terrorist financing measures

# India

## Mutual Evaluation Report

September 2024

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org.**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

**This assessment was adopted by the FATF at its June 2024 Plenary meeting.**

Citing reference:

FATF/OECD – APG, EAG (2024), *Anti-money laundering and counter-terrorist financing measures – India,*
Fourth Round Mutual Evaluation Report, FATF, Paris
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/Mer-India-2024.html



Photo Credit - Cover: © PTI/Shahbaz Khan

# *Table of Contents*

# *Executive Summary*

1. This report summarises the AML/CFT measures in place in India as at the date of the on-site visit from 6 to 24 November 2023. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of India's AML/CFT system and provides recommendations on how the system could be strengthened.

## Key Findings

- Authorities have a strong understanding of ML risks, and operational authorities have a sophisticated understanding of TF risks. Understanding of ML threats arising from trafficking in human beings and migrant smuggling and ML/TF risks from smuggling and dealing in precious metals and stones can be further developed. Effective domestic coordination and cooperation on AML/CFT issues occurs at both the policy and operational levels.
- LEAs routinely access and use financial intelligence and other relevant information in investigations related to ML, predicate offences and TF. The FIU's analysis and dissemination support the operational needs of competent authorities to a significant extent, although there are low levels of requests from some LEAs, including to support tracing of criminal assets. Nevertheless, significant quantities of proceeds are attached (seized) by LEAs at the early stages of investigations, helping deprive criminals of proceeds and helping prevent asset flight.
- Potential ML is identified systematically via multiple routes, and although LEAs are carrying out parallel financial investigations for underlying predicate offences, their effectiveness appears to be affecting detection to some extent. The Enforcement Directorate is able to investigate and prosecute more complex cases, and pursues ML related to fraud and forgery in line with predicate crime risks, but less so in trafficking in human beings and migrant smuggling, and drug trafficking. The multiple sources of beneficial ownership information available have helped in investigations, although it is not clear to what extent the register of significant beneficial owners is fully populated.
- The number of ML convictions has been significantly impacted by a series of constitutional challenges (settled in 2022) with many cases pending trial and the saturation of the court system observed. Although numbers of

prosecutions and convictions have started to increase, the backlog of pending cases remains considerable, with a large number of accused persons awaiting conclusion of their trials. This also impacts the extent to which confiscation of criminal proceeds is carried out, in particular the ML cases that the ED is responsible for, although India has confiscated proceeds via non conviction-based confiscation including in some significant cases.

- TF investigations are broadly conducted in line with the risks identified and case studies reflect India's ability to conduct complex financial investigations and identify financial flows. However, there are significant delays in prosecutions, resulting in a high number of pending cases and accused awaiting trial. India's emphasis on disruption and prevention of terrorism and TF is broadly consistent with risk, including through asset seizures of designated individuals and entities. Measures relating to the prevention of the NPO sector from abuse are not calibrated with risks.
- There is a good general understanding of risks and obligations as well as application of mitigating measures in the financial sector. The application of preventive measures is steadily progressing with the recent inclusion of VASPs and many DNFBP sectors as reporting entities, although major improvements are still needed. Suspicious transaction reporting by some FI sub-sectors appears limited and DNFBPs are yet to detect suspicious activity and file STRs in a significant way.
- Checks to prevent criminals from entering the financial, VASP and DNFBP sectors are broadly adequate, except for the DPMS sector and some non-banking FIs, and checks in many sectors are insufficient to spot criminal association. Risk understanding and corresponding risk-based supervision is uneven amongst supervisors, although more positive findings are observed for the financial supervisor responsible for the most material sectors. Sanctions applied were not always proportionate and dissuasive. For the DNFBPs sector, supervision is less developed or yet to commence, including in high-risk sectors. The ML/TF risks of the DPMS sector are not sufficiently mitigated by a prohibition on cash transactions under tax law.
- India has taken recent steps to improve MLA coordination within India and the timeliness of responses to formal requests for international cooperation. Competent authorities seek international cooperation where relevant, although some improvements can be made to the quality of requests. LEAs and FIU-IND proactively seek and provide informal cooperation with foreign counterparts.

## Risks and General Situation

2. India's main sources of money laundering originate from within India, from illegal activities committed within the country. These proceeds may be laundered within India, laundered abroad, or laundered abroad and returned to India for re-integration into the licit economy. Consistent with the outcomes of the NRA, India's largest money laundering risks are related to fraud including cyber-enabled fraud, corruption, and drug trafficking.

3. India faces a disparate range of terrorism threats, categorised into six different theatres. These can be summarised as theatres associated with ISIL or AQ linked extremist groups active in

and around Jammu and Kashmir, whether directly or via proxies or affiliates, as well as other separatist movements in the region; other ISIL and AQ cells, their affiliates, or radicalised individuals in India; regional insurgencies in the Northeast and North of India; and left-wing extremist groups seeking to overthrow the government. The most significant terrorism threats appear to relate to ISIL or AQ linked groups active in and around Jammu and Kashmir.

4. Terrorist financing risks are generally closely linked with terrorism risks, with flows of funds or provision of other assets constrained to within India or surrounding countries.

## Overall Level of Compliance and Effectiveness

5. India has implemented an AML/CFT system that is effective in many respects. Particularly good results are being achieved in the areas of ML/TF risk understanding; national coordination and cooperation; use of financial intelligence for ML, predicate offences and TF investigations; depriving criminals of their assets; preventing misuse of legal structures; the implementation of targeted financial sanctions related to proliferation; and international cooperation. However, major improvements are needed to strengthen prosecution of ML and TF, protecting the non-profit sector from terrorist abuse, supervision and implementation of preventive measures.

6. Many positive developments have taken place in the last two to three years before the on-site visit, and while some initiatives are beginning to show results (e.g., increases in ML investigations, improvements to the timelines for incoming MLA requests, the implementation of a new mechanism of TFS for PF), others have been too recent and require an appropriate period of time to be operational and lead to changes in the effectiveness of the system (e.g., DNFBP and VASP supervision).

7. India has achieved strong results in its technical compliance with the FATF Standards. The remaining areas requiring significant improvement are risk-based measured to protect NPOs, establishing due diligence requirements on domestic PEPs and supervision of DNFBPs.

### *Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)*

8. Authorities in India have a strong understanding of ML risks and in particular, law enforcement and intelligence authorities involved in CFT have a sophisticated understanding of TF risks as reflected in the 2022 NRA, various sectoral risk assessments, policies, and cases. Consistent with the risks identified in the NRA, India has implemented a broad range of policy, operational and legislative measures to mitigate these risks. A key strength of the Indian system is its continuous domestic coordination and cooperation on AML/CFT issues at both the policy and operational levels at the central and state levels which has improved since the last assessment.

9. There are some shortcomings in risk understanding, particularly relating to ML threats arising from trafficking in human beings and migrant smuggling, and ML/TF risks from smuggling and dealing in precious metals and stones, where understanding can be further developed. A more detailed action plan that provides more granular mitigation measures, which lays out clear priorities and benchmarks implementation, would strengthen responses.

10. The conclusions of the non-public NRA and sectoral risk assessments have been communicated to many of the reporting entities across different states. However, there remains a significant volume of reporting entities that have not been engaged.

### *Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)*

11. LEAs and intelligence agencies routinely access and use financial intelligence and other relevant information in investigations related to ML, predicate offences and TF. The FIU's (FIU-IND) analysis and dissemination support the operational needs of competent authorities to a significant extent. The lower levels of requests from some LEAs, as well as for tracing and attaching assets, supports the need to improve the feedback framework between the FIU and end users.

12. The Enforcement Directorate (ED), the sole competent authority mandated to investigate ML activities, is able to investigate and prosecute complex ML activity. While LEAs are routinely identifying proceeds when investigating predicate offences, it is not clear it is sufficiently carrying out effective parallel financial investigations and detecting potential money laundering cases.

13. The ED pursues ML related to fraud and forgery in line with predicate crime risks to a large extent, but less so with other offences in particular trafficking in human beings and migrant smuggling, and drug trafficking. The number of ML convictions over the last five years has been impacted by a series of constitutional challenges (resolved in 2022) and the saturation of the court system. Although the number of prosecutions and convictions have started to increase, the backlog of pending cases remains considerable.

14. Competent authorities responsible for asset recovery have a broad set of powers available, enabling them to seize and confiscate property of suspects in a wide variety of circumstances. Operationally and as a matter of policy, the ED makes significant use of powers to attach (seize), depriving criminals of proceeds and helping prevent asset flight, resulting in assets valued at EUR 9.3 billion attached over the last five years.

15. Confiscations based on convictions for ML have amounted to EUR 4.4 million over the evaluation period, which is inconsistent with risk, impacted by the cases pending before the courts. Non-conviction-based confiscation for ML, amounting to EUR 1.84 billion, has been used during the period on a small number of cases, some of which are significant.

16. India has a system of capital controls and has in place a declaration system for incoming cross-border movements and a disclosure system for outgoing movements. However, the focus on cross-border cash movements is directed towards identifying breaches of capital controls rather than AML/CFT concerns.

### *Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)*

17. Indian authorities have demonstrated a good understanding of both current and emerging TF threats and risks in different theatres of risk in the country, and investigations are broadly conducted in line with the risks identified. Case studies provided reflect India's ability, in particular the National Investigative Agency (NIA) and ED, to conduct complex financial investigation and identify money trails to support the investigation and prosecution of terrorist activity and TF.

18. However, statistics and case studies also reflect significant delays in prosecutions both at the NIA and State level, resulting in a high number of pending cases and accused persons in judicial custody waiting for cases to be tried and concluded. Based on the number of open cases, it could not be concluded that TF offenders were being successfully convicted during the evaluated period.

19. India's strong emphasis on disruption and prevention mechanisms for terrorism and TF, including through asset seizures of designated individuals and entities, is in line with TF risks overall. However, measures relating to preventing the NPO sector from being abused for TF, are not calibrated to the subset of NPOs identified as at risk for TF abuse. While there is ongoing

engagement with NPOs, this is not sufficiently coordinated amongst the different government authorities and more specific TF risks relating to NPOs are not adequately communicated.

20. India has an interagency framework to designate entities for UNSCRs, which it uses to designate terrorists and terrorist organisations. However, the time and manner in which the obligations to freeze should be implemented without delay, is not always clear. In practice, established reporting entities utilise commercial sanction screening software to do this, although more recently regulated DNFBPs require more support to enable them to better implement their TFS obligations.

21. Since January 2023, India has in place a more streamlined framework to implement PF TFS obligations without delay under the WMD Order. In addition, there is a communication mechanism that relays listings to reporting entities through their respective regulators without delay and established FIs and VASPs understand their PF TFS obligations, relying on sanction screening software for this. DNFBPs do not have the same level of awareness or structures. Prior to January 2023, while there was a broad prohibition not to finance sanctioned persons and entities under the WMD Act, there was no clear articulation of the obligation to freeze funds and assets without delay.

22. To date, there have been no TFS matches with designated lists under UNSCR 1718 reported to MEA or FIU-IND, which is consistent with the exposure of India to PF activity.

### *Preventive measures (Chapter 5; IO.4; R.9–23)*

23. There is a good general understanding of ML/TF risks and application of mitigating measures in the financial sector, in particular by commercial banks, but less so for some other FIs including in the foreign exchange sector and cooperative banks. CDD and enhanced measures are being applied but the identification of beneficial owners is an area for improvement. All sectors seem to apply EDD to domestic PEPs, notwithstanding the absence of a legal requirement, but there are some inconsistencies on the breadth of domestic PEPs being identified.

24. Implementation of AML/CFT requirements by VASPs and DNFBPs is in its early stages. VASPs generally demonstrated a good understanding of risks and obligations, and seem to apply preventive measures to a reasonable extent. Despite the lack of supervision for most DNFBPs sectors, DNFBPs seem to understand their obligations and ML risks, commensurate with their materiality and size of business operations. Some improvements are required in relation to TF risk understanding and TFS freezing obligations.

25. Suspicious transaction reporting by some FI sub-sectors appears low (including non-financial banking companies, the Department of Post and rural banks) and DNFBPs are yet to detect and file STRs in a significant way.

### *Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)*

26. Licencing, registration and fitness and probity checks to prevent criminals from entering the financial, VASP and DNFBP sectors are broadly adequate, although less so for DPMS and some smaller FIs. There are insufficient checks to identify criminal associates across many sectors.

27. RBI, the financial supervisor of the banking sector and other material FIs, has a good understanding of inherent ML risks and a reasonable understanding of TF risks, adopting a risk-based approach to supervision for the most material sectors. The supervision of the Money Transfer Services Scheme (MTSS) sector, a type of MVTS identified in the NRA as posing TF risks, is not sufficiently calibrated to the risks of the sector.

28. For the VASP sector, whilst risk-based supervision has commenced, supervisory capacity appears limited considering the complexity and growing nature of the sector. For the DNFBP sector,

supervision is less developed (except for casinos) with limited or no capacity to supervise and monitor compliance with AML/CFT obligations.

29. Financial sanctions imposed by supervisors were generally limited in number and value. Business restrictions imposed by the RBI in a case of systemic failure appear more dissuasive. The enforcement action by FIU-IND against FIs that have committed serious systemic failures in STR reporting has raised the effectiveness of the sanctioning regime to some extent.

30. As a result of tax law provisions relating to cash threshold prohibition, the DPMS sector falls outside the scope of preventive measures. The prohibition is monitored largely through an external audit mechanism with reports prepared by an external accountant and tax inspections conducted by CBDT. However, the adequacy of the compliance monitoring of the DPMS sector with the threshold prohibition is uncertain and there are doubts on the dissuasiveness of the penalty provisions. This raises doubts as to whether the ML/TF risks in the sector are effectively mitigated by the prohibition.

### *Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)*

31. India has a good understanding of the inherent vulnerabilities associated with different types of legal persons, although there is a need for better assessing residual risks posed by informal nominee arrangements, which is important in the country risk and context.

32. India has taken a number of positive steps to enhance the transparency of information on legal persons and arrangements. This includes conducting an intensive campaign to remove shell companies from its company registry, and implementing a public registry of "significant beneficial owners" of legal persons that have declared having a more complex control structure. The latter contains a small proportion of legal persons in India. A central KYC registry, containing BO information of legal persons and arrangements that have a relationship with an Indian financial institution, provides another source of BO information. Indian competent authorities have been able to access basic and BO information in cases from a variety of sources.

33. There has been a focus on striking off non-compliant companies and shell companies in the MCA registry. However, the limited number and size of sanctions imposed for more serious non-compliance may not have the dissuasive effect needed to prevent non-compliance in all circumstances.

34. India relies on registers of public trusts, tax law and CDD requirements for the availability of information on legal arrangements; however, the fragmented way information is kept in relation to public trusts and the very recent CDD obligations for professional trustees limits availability to some extent.

### *International cooperation (Chapter 8; IO.2; R.36–40)*

35. India has an appropriate legal framework in place to support MLA and extradition and has recently taken important steps, introducing and implementing updated guidelines and an online portal for coordination and prioritisation, to improve the coordination and timeliness of responding to requests for international cooperation. Seeking formal international cooperation where necessary is a standard component of ML/TF investigations in India. Requests have been made in keeping with the country's risk profile but some improvements could be made to the quality of these requests.

36. LEAs and the FIU proactively seek and provide informal cooperation with foreign counterparts. This cooperation has assisted authorities in India to advance ML/TF investigations. Financial supervisors have sought and provided international cooperation, although this has

generally been limited to the provision of information related to fit and proper checks, including basic and beneficial ownership information.

### Priority Actions

- India should undertake more comprehensive financial network analysis especially on ML techniques associated with trafficking in human beings and migrant smuggling, to develop its understanding of the ML risks associated with these.
- India should enhance the capacity of LEAs to enable them, to more effectively pursue parallel financial investigations into proceeds generating predicate offences, including by FIU-IND working with LEAs to enhance use of financial intelligence in support of complex financial investigations and asset tracing.
- India should aim to reduce the number of pending trials in ML cases – both for new trials and for the backlog, addressing the low number of convictions associated ML cases and increasing conviction-based confiscation, by making major changes to increase the capacity of the court system, and potentially the capacity of the ED.
- India should make major changes to address delays relating to the prosecution of TF cases, so as to improve the timeliness of their judicial disposal and clear the serious backlog of unconcluded TF prosecutions.
- India should improve its framework for implementing TFS so that it is clear that all natural and legal persons are obliged to freeze funds and assets without delay, streamline the process for communicating TFS listings so that all reporting entities receive the updates without delay in line with the requirements of R.6, and ensure that outreach to reporting entities is regular and sustained.
- India should ensure that CFT measures aimed at preventing the NPO sector from being abused for TF are implemented in line with the risk-based approach, including by conducting outreach to NPOs on their TF risks. Outreach should be conducted in a more focused coordinated and risk-based manner by the relevant competent authorities, ensuring NPOs at risk of TF abuse enhance their understanding of TF risks, including the sources, channels and end-use of funds as per their respective theatre.
- India should address technical compliance deficiencies in relation to Recommendation 12, establishing clear obligations concerning domestic PEPs. Reporting entities should improve identification of domestic PEPs and take risk-based enhanced measures in relation to them.
- India should develop the capacity of all DNFBP supervisors that have been recently incorporated so that they apply AML/CFT supervisory actions to their sectors on a risk-sensitive basis. DNFBPs should improve detection of suspicious transactions as well as increase the quantity of STRs, particularly by high-risk sectors, when suspicious activity is detected.
- In view of the risks presented by the MTSS Scheme , India should prioritise the risk-based supervision of the sector, including by RBI working with MTSS

principals and Indian agents to increase the level of risk understanding of ML/TF risks and AML/CFT obligations.

- In view of the risk and materiality of the DPMS sector, India should enhance measures to prevent criminals or their associates from participating in the sector and enhance monitoring of the sector's compliance with mitigating measures, including enforcement of the cash prohibition.
- India should enhance monitoring of the MCA registry to ensure the availability of adequate, accurate and up-to-date basic and BO information on legal persons.

## Effectiveness & Technical Compliance Ratings

### Table 1. Effectiveness Rating

| IO.1 - Risk, policy and co-ordination | IO.2 International co-operation | IO.3 - Supervision | IO.4 - Preventive measures | IO.5 - Legal persons and arrangements | IO.6 - Financial intelligence |
|---|---|---|---|---|---|
| Substantial | Substantial | Moderate | Moderate | Substantial | Substantial |
| **IO.7 - ML investigation & prosecution** | **IO.8 - Confiscation** | **IO.9 - TF investigation & prosecution** | **IO.10 - TF preventive measures & financial sanctions** | **IO.11 - PF financial sanctions** | |
| Moderate | Substantial | Moderate | Moderate | Substantial | |

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

### Table 2. Technical Compliance Ratings

| | | | | | |
|---|---|---|---|---|---|
| **R.1** - assessing risk & applying risk-based approach | **R.2** - national co-operation and co-ordination | **R.3** - money laundering offence | **R.4** - confiscation & provisional measures | **R.5** - terrorist financing offence | **R.6** - targeted financial sanctions – terrorism & terrorist financing |
| LC | C | LC | LC | LC | LC |
| **R.7**- targeted financial sanctions - proliferation | **R.8** -non-profit organisations | **R.9** – financial institution secrecy laws | **R.10** – Customer due diligence | **R.11** – Record keeping | **R.12** – Politically exposed persons |
| LC | PC | C | LC | C | PC |
| **R.13** – Correspondent banking | **R.14** – Money or value transfer services | **R.15** –New technologies | **R.16** –Wire transfers | **R.17** – Reliance on third parties | **R.18** – Internal controls and foreign branches and subsidiaries |
| C | LC | LC | C | LC | LC |
| **R.19** – Higher-risk countries | **R.20** – Reporting of suspicious transactions | **R.21** – Tipping-off and confidentiality | **R.22** - DNFBPs: Customer due diligence | **R.23** – DNFBPs: Other measures | **R.24** – Transparency & BO of legal persons |
| LC | LC | C | LC | LC | LC |
| **R.25** - Transparency & BO of legal arrangements | **R.26** – Regulation and supervision of financial institutions | **R.27** – Powers of supervision | **R.28** – Regulation and supervision of DNFBPs | **R.29** – Financial intelligence units | **R.30** – Responsibilities of law enforcement and investigative authorities |
| LC | LC | C | PC | C | LC |
| **R.31** – Powers of law enforcement and investigative authorities | **R.32** – Cash couriers | **R.33** – Statistics | **R.34** – Guidance and feedback | **R.35** – Sanctions | **R.36** – International instruments |
| LC | LC | C | LC | LC | C |
| **R.37** – Mutual legal assistance | **R.38** – Mutual legal assistance: freezing and confiscation | **R.39** – Extradition | **R.40** – Other forms of international co-operation | | |
| LC | LC | C | LC | | |

Note: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

# MUTUAL EVALUATION REPORT

## Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 6 to 24 November 2023.

The date of the evaluation was postponed due to the COVID-19 pandemic.

The evaluation was conducted by an assessment team consisting of:

- Mr. Igor Alekseev, Rosfinmonitoring, Financial Intelligence Unit of the Russian Federation (FIU expert).
- Mr. Sauod Almutawa, Dubai Police, United Arab Emirates (legal and law enforcement expert).
- Ms. Sandra Garcia, United States of America Department of the Treasury (policy and sanctions expert).
- Ms. Juliana Petribú Gorenstein, Central Bank of Brazil (financial expert).
- Ms. Alison Kelly, HM Treasury, United Kingdom (law enforcement expert).
- Mr. Phineas Rameshovo Moloto, Financial Intelligence Centre of South Africa (financial expert).
- Mr. Masayuki Nakamura, Japan Ministry of Finance (policy expert).

The assessment team was supported by Mr. Neil Everitt, Ms. Ravneet Kaur and Ms. Renata Teixeira from the FATF Secretariat, Ms. Melissa Sevil from the APG Secretariat, and Mr. Sergey Teterukov from the EAG Secretariat.

The report was reviewed by the IMF, Mr. Tiago Lambin (Institute of Public Markets Real Estate and Construction, Portugal), Mr. Robert Milnes (Department of Internal Affairs, New Zealand) and Mr. Firuz Murodov (National Bank of Tajikistan).

India previously underwent a FATF Mutual Evaluation in 2010, prepared using the 2004 FATF Methodology.

That Mutual Evaluation concluded that the country was compliant with four Recommendations; largely compliant with 25; partially compliant with 15; and non-compliant with four. One recommendation was considered not applicable. India was rated compliant or largely compliant with seven of the 16 Core and Key Recommendations.

India was placed on the regular follow-up process upon adoption of its 2010 mutual evaluation. In context of its application to become a member of the FATF, an action plan to improve the compliance of its AML/CFT regime was adopted alongside its mutual evaluation in 2010 and

India became a member. India subsequently reported progress against its action plan at FATF Plenary held between June 2010 to June 2013. India was removed from the regular follow-up process in June 2013 on the basis of a desk-based review, finding that India had reached a satisfactory level of compliance with all of the Core and Key Recommendations.

# Chapter 1. ML/TF RISKS AND CONTEXT

## *Geography and population*

37. The Republic of India (India) covers an area of 3.29 million square kilometres, sharing land borders with Pakistan and Afghanistan in the west; Bangladesh and Myanmar in the east; and Nepal, China, and Bhutan in the north. India also has maritime borders with Indonesia, Thailand, Sri Lanka and the Maldives. India has rich and varied natural biodiversity,[1] with approximately 24% of territory as forest cover, largely owned or managed by the Government.[2]

38. India's population is the largest in the world, with its 1.4 billion inhabitants representing around 18% of the world's population.[3] India is densely populated,[4] with around a third of the population living in cities,[5] and has the world's largest aggregate diaspora, with more than 32 million Indian nationals living in other countries,[6] including more than 4.5 million in the United States, 4.1 million in Saudi Arabia, 3.4 million in the UAE and 2.9 million in Malaysia.[7]

39. India is a culturally diverse, multi-ethnic country. There is no single national language in India, with 22 official languages, 122 major language groups, and several thousand dialects spoken. There are also 705 ethnic groups officially recognised as Scheduled Tribes, each with their own identity. While a significant majority of India's population are Hindus (80%), there are also large populations of Muslims (14%), Christians (2%), Sikhs (2%), and Buddhists (1%).

## *Legal and administrative system*

40. India has a federal system of government consisting of the Union or Central Government, and State Governments. The Constitution (adopted in 1950) provides for a bicameral parliament and three branches: the executive, legislative and judiciary. Alongside the elected Central Government, there are elected Governments in the 28 States and eight Union Territories. The Indian Constitution assigns the responsibilities between the Central and State Governments. English and Hindi are the Official languages of the Government. AML/CFT policy and enforcement of the

---

1 India is recognised by the UN Convention on Biodiversity as 'megadiverse,' as 7-8% of the world's recorded species live in India. It also has three of the world's 34 biodiversity 'hotspots.' See www.cbd.int.

2 See Forest Survey of India, Ministry of Environment Forest and Climate Change (2021) available from www.fsi.nic.in.

3 UN Department of Economic and Social Affairs (UN DESA) policy brief no.153, April 2023. Available from www.un.org.

4 Approximately 473 persons per square kilometre according to the most recent data from the World Bank data, available from 2021. Excluding offshore centres and small states or jurisdictions with a population of less than 1 million, India was the most 7th most densely populated Nation according to World Bank data after Bahrain, Bangladesh, Rwanda, South Korea, Lebanon and Burundi.

5 According to World Bank development indicators 2022.

6 13.5 million non-resident Indians, and 18.7 million persons of Indian Origin according India's Ministry of External Affairs as of 2018.

7 Other countries with populations of more than 1 million are Myanmar (2 million), the UK (1.9 million), Canada (1.9 million), Sri Lanka (1.5 million), South Africa (1.5 million) and Kuwait (1 million). India's Ministry of External Affairs (2018).

1

legislative framework concerning AML/CFT, are predominantly exercised at the Central Government level.

41. Responsibility for administration lies with Ministers of the Central and State Governments, supported by the permanent civil service, with the State continuing to play an important role in the economy. Members of the civil service are posted at various levels in Central, State, District and Local governments, performing a wide range of important administrative functions, including maintenance of law and order, land and revenue administration, taxation and management of public sector agencies. All civil servants must follow a central set of rules governing their conduct.

42. India has a common law legal system. The Indian Judiciary's function is to administer justice independently. The Supreme Court of India is the highest judicial authority and has the power of judicial review to interpret the Constitution and strike down laws that are in violation with it. The Supreme Court, along with the High Courts (Courts of Appeal), Subordinate Courts, Appellate Tribunals and Tribunals, provides for a single unified system to administer both Union and State Law.

## ML/TF Risks and Scoping of Higher Risk Issues

### *Overview of ML/TF Risks*

43. Given the country's size, aggregate ML risks are considered similar to global ML trends for low-medium income countries that are not international financial centres. The specific risks are described in the following section. The size of the country also means that there is regional variation in the type and extent of the different types of ML and TF risks faced within the country, a factor which has been integrated into the methodology of the latest NRA conducted by India.

44. In general, India is not an attractive destination country for criminal proceeds, relative to the size of its economy and population, although cross-border risks for ML and TF (with funds moving into and out of the country) are present as explained below. Overall, the main sources of money laundering originate from within India, from illegal activities committed within the country. These proceeds may be laundered within India, laundered abroad, or laundered abroad and returned to India for re-integration into the licit economy.

45. India has suffered from the effects of terrorism consistently since its independence in 1947. India faces a disparate range of terrorism threats, categorised by India into six different theatres. These can be summarised as theatres associated with ISIL or AQ linked extremist groups active in and around Jammu and Kashmir, whether directly or via proxies or affiliates, as well as other separatist movements in the region; other ISIL and AQ cells, their affiliates, or radicalised individuals in India; regional insurgencies in the Northeast and North of India; and left-wing extremist groups seeking to overthrow the government. The most significant terrorism threats appear to relate to ISIL or AQ linked groups active in and around Jammu and Kashmir.

46. Terrorist financing risks are generally closely linked with terrorism risks, with flows of funds or provision of other assets constrained to within India or surrounding countries.

### *Country's Risk Assessment & Scoping of Higher Risk Issues*

47. India had drawn upon a range of sectoral risk assessments to identify and understand its ML/TF risks. India's second National Risk Assessment (NRA) adopted in 2022 builds on the conclusions of the previous NRA concluded in 2011. Between 2011 and 2022, and more recently

outside of the NRA, several other thematic assessments have been conducted. None have been publicly disseminated except for the White Paper on Black Money report.[8] These include:

- **White Paper on Black Money** (2012) that assessed the magnitude of 'black money' dissipated from India, focusing on proceeds dissipating from India associated with the illegal drug trade, terrorism, corruption, and higher end tax evasion). Analysis covered assessments of vulnerable sections of the economy.[9]
- **The Special Investigation Team on Black Money** produced eight reports between 2014 and 2022 that covered/focused on illicit movement of funds out of India, of money on which income and other taxes have not been paid.
- **Risks, Trends and Methods Report** (2019) assessed the impact of the mitigation measures instituted after the 2011 NRA on the financial sector and identified residual risks. This report contains granular data points such as the effectiveness of supervision, availability and effectiveness of sanctions and border controls and integrity and AML knowledge of bank staff.
- **A series of ad hoc sectoral risk assessments** were carried out in 2022 and 2023. Specific assessments were made on for Accountants, Lawyers and TCSPs (2022) to examine their ML/TF risk exposure, Virtual Assets and Service Providers (2022) and the Postal Sector (2023), to examine ML/TF risks associated with these sectors and the Real Estate Sector (2023) to understand the real estate market and the risks associated with them. Assessments were also carried out on Legal Persons and Arrangements (2023) to assess the risks relating to different types of legal persons and arrangements in the country and examine the mitigating measures implemented, and NPOs for TF abuse (2023) that assessed the risks of NPOs being abused for TF in the different TF theatres identified in the NRA and TF risk assessment (2022) (see above).

48. The 2022 NRA represented a significant exercise that involved a large number of competent authorities as well as private sector participants. The process was administered by a Joint Working Group (JWG), overseen by an inter-ministerial committee. Constituents of the JWG included a broad range of government agencies (see table 2.1).

49. The NRA uses a hybrid of the first- and second-generation World Bank tools as a basis, applying a matrix approach to assign scores to different risks as a function of four factors – threat, vulnerability, consequence and mitigation. The 2022 NRA exercise includes analysis of ML threats posed by various predicate offences (considering eight factors), vulnerabilities of India's systems to such threats, and specific threat and vulnerabilities in various sectors. The sectoral risk assessment sections of the 2022 NRA cover FIs, DNFBPs, and financial inclusion services and products. Data points are drawn from a range of quantitative and qualitative sources. Quantitative sources included the incidence of the predicate crime reported, quantum of the proceeds of crime generated from the offence, impact of the offence on citizens, security and integrity of India, how widespread incidence of the crime is across the country (regional variation), complexity of the techniques of ML, extent of cross-border movement of the proceeds as well as the involvement of politically exposed persons (PEPs) in the offences. Qualitative sources included interviews and inputs from law enforcement and other competent authorities on money laundering methods and

[8] Published on the Department of Revenue website.

[9] Including the real estate sector, the bullion and jewellery market, financial markets, public procurement, non-profit organisations, external trade, international transactions involving tax havens, and the informal service sector. The need for more research on the misuse of corporate structures was also cited.

trends, analysis of MLA and Egmont requests sent and received, typologies found in predicate offence and ML investigations, and feedback from the private sector to inform product and sector risk understanding and emerging risk. Although the methodology does not directly consider STR data, STR data is used to verify the conclusions in the report.

50. Vulnerabilities are based on the assessment of the capabilities of national AML controls in place in the different sectors (sectoral risks) and the existence of any remaining regulatory gaps with input from LEAs and FIU-IND, case studies, data from NCRB and ED and examination of the legal framework. Sub-groups headed by a sector regulator or expert utilised expert evidence including feedback from the private sector, data, and contextual factors specific to each sector to arrive at a vulnerability score. Feedback from the private sector was taken through three structured forums: (1) FIU-India Initiative for Partnership in AML/CFT (F-PAC), which is hosted by FIU-IND and has RBI and forty-seven systematically important reporting entities; (2) deliberation stemming from various Working Groups formed by FIU-India for formulating and updating of Red Flag Indicators (RFIs); and (3) RBI led sector-specific working groups for the banking sector and Other Financial Institutions (OFIs) for the vulnerability assessment part of the 2022 NRA.

51. ML threats and vulnerabilities are ultimately given a rating within five classifications (low, medium-low, medium, medium-high, high) resulting in a residual rating based on the same five-point scale. The full NRA has not been published for wider public, although relevant extracts have been shared with reporting entities as part of presentations taken place via outreach and through the FIU FINGATE portal for reporting entities registered with the FIU, where conclusions of the NRA were compiled into a PowerPoint presentation and a digital alert was sent to compliance officers of registered FIs and DNFBPs on the portal.

52. ML threats presenting high and medium risks are fraud – primarily bank fraud, investment frauds and cyber-enabled fraud; forgery; illicit trafficking in narcotics and psychotropic substances; and corruption. Hawala, cash couriers, shell companies, offshore instruments[10] and trade-based money laundering (TBML) are assessed as the channels for laundering proceeds. The purchase of real estate, precious stones and use of third-party bank accounts are also identified as goods and services that are vulnerable to money laundering. Sectoral risk assessments embedded in the 2022 NRA or conducted shortly before or after it found that the ML threats related to the real estate, banking, and securities, as high, medium-high and medium respectively, but after considering vulnerabilities, the overall risk levels are medium except for real estate which is medium-high.

53. The assessment of TF risk in the NRA is based on a separate, more detailed TF risk assessment, concluded in 2022. The TF Risk Assessment relied more heavily on results of intelligence and investigations, following a different methodology from that used for ML. It focuses on the source, channels and theatres of terrorism relying on incidence reports, intelligence, the content of investigations and prosecutions and qualitative analysis by operational experts over several years to understand the movement of money into and within a set of six geographic and thematic 'theatres' of terrorist activity, summarised above. Case studies dating from 2011 to 2022 were analysed. The mechanisms used to raise, move and use terrorist funds or other assets were found to vary between 'theatre' (see above). Sources from outside the country and arms trafficking are assessed as the highest risk sources for raising funds across theatres, while Hawala and cash couriers are the methods assessed as highest risk for moving funds and other assets. Within specific theatres, banking and MTSS scheme were also considered to be high risk. India also assessed that it faces emerging risks related to growing virtual asset misuse especially from jurisdictions that do not regulate VASPs for AML/CFT and offshore financial centres.

[10] Considered by India in context of the NRA as a variety of instruments associated with tax havens, including Special Purpose Vehicles, trusts and foundations used to hide beneficial ownership information.

54. Although not required under the current FATF Methodology, India also assessed its vulnerability for PF in the 2022 NRA, focusing on mitigation controls including its regulatory system for internationally controlled items, and compliance with relevant UNSCR to prevent WMD proliferation and PF.

55. The assessment team agreed with the majority of the conclusions of the NRA, in particular those described in paras above, and that these conclusions were based on a set of thorough processes and mechanisms to gather and evaluate information, resulting in a set of reasonable insights. The assessment team however considered that the financial component and ML techniques associated with trafficking in human beings and migrant smuggling as well as the ML risks associated with smuggling and dealing in precious metals and stones should be further examined by India. In particular, concerning the possibility that these may represent higher risks with criminal networks operating cross border not being investigated and captured in law enforcement reporting (See IO.1).

56. In deciding which issues to prioritise for increased focus, the assessors reviewed material provided by India on their national ML/TF risks (as outlined above), and information from reliable third-party sources. The assessment team focused on the below priority issues which are broadly consistent with those identified in the NRA, and in context of the higher risks described above. Other areas of risk that were provisionally considered were tax evasion, environmental crime and organised crime. During the onsite visit, the assessment team considered India's approach to pursuing tax evasion offences largely under domestic tax laws and strong financial transparency measures, and pursuit of proceeds when they are laundered abroad. Action taken on predicate environmental crimes were considered since India noted that environmental crime presented low ML risks as a result of these actions. Threats related to organised crime were considered through the various predicate crime types that were more likely to involve organised criminal groups e.g., narcotic offences, trafficking in human beings and migrant smuggling, smuggling (including in precious metals ad stones). Analysis is included in IO.1.

### *Money Laundering*

- **Identification and execution of ML cases.** In its last evaluation in 2010, India had not achieved a successful conviction for ML. The overarching AML legislative framework in India has also been subject to legal challenge (see below). India also appears to continue to face challenges with corruption, at least to some extent. Assessors considered how India has built knowledge and expertise amongst law enforcement authorities, prosecutorial authorities and the judiciary since 2010, and how it is prioritising cases on a day-to-day basis in context of the risks it faces especially where they relate to areas of higher risk exposure.
- **Misuse of legal persons**. The NRA identifies the use of shell companies is a preferred route for ML involving significant sums, especially for proceeds of fraud offences corruption and tax crimes. Risks involve the laundering of proceeds outside of India using corporate structures, with a high-risk of dissipation to overseas "secrecy jurisdictions." Assessors focused on the coverage and supervision of professional gatekeepers of these structures under India's AML/CFT system, the implementation of preventative measures and detection of suspicious activity, beneficial ownership transparency and international cooperation.

1

### *Terrorist financing*

- **TF risks associated with NPOs.** NPOs are identified in the NRA as being misused to raise funds for terrorist activity to differing extents, depending on the theatre and type of terrorist organisation. Assessors focused on how NPOs at risk are identified and monitored, the nature of outreach conducted, information shared, and action taken by the authorities and its consistency with ensuring legitimate work carried out by NPOs is not disrupted.

## *Money Laundering and Terrorist Financing*

- **Use of cash to move illicit funds.** Although digital payments and financial inclusion have reduced the population's dependence on cash (see below), a significant proportion of the population remains outside the formal banking system. The use of cash couriers within the country and across borders is an identified risk in the NRA for both ML and TF, while India has extensive land and maritime borders (see above). Assessors considered how well the authorities understand and mitigate risks associated with the use of cash and movement of illicit flows entering and leaving India.
- **Banking Sector.** Given the size of the sector and identified risks in the NRA,[11] assessors focused on the extent to which preventive measures are being implemented by the sector and how well the sector is being supervised for AML/CFT.
- **Remittances and Alternative Remitters**. MVTS sectors are considered more susceptible for ML and TF in the NRA, with Hawalas in particular identified as involved in the movement of funds within and across several different theatres. Assessors considered how effectively customer due diligence and other controls are applied within the licenced sector and whether authorities are effectively identifying and shutting down unlicenced providers.
- **Vulnerability of new Technologies**. India has introduced widely adopted digital infrastructure for payment services and personal identification. The national policy on VASPs and corresponding AML/CFT framework is being implemented. The rapid pace of development of the fintech sector in India also presents vulnerabilities, as India seeks to address gaps and implement new requirements as new products and services are being introduced, for example recent changes in licencing to capture payment intermediaries.[12] [13] The assessors considered the extent to which these vulnerabilities are being exploited and how risks are being mitigated by India.
- **India's International Financial Centre**. Assessors considered whether the new products and services offered by the firms in India's International Financial Services Centre (IFSC), created in 2011, pose vulnerabilities; and how the IFSC Authority (IFSCA) has built its capability relative to the challenges of a new

[11] Quantum of transactions relative to other sectors of the economy, complexity of transactions involved and the likelihood that any ML case would involve the banking sector in placement, layering and/or integration of the proceeds of crime.

[12] ML/TF Sectoral Risk Assessment for VA & VASP 2022.

[13] India is one of the fasted growing Fintech markets in the World. See India's National Investment Promotion Agency, with a market size of USD 50 billion (2021). See www.investindia.gov.in.

supervisor overseeing firms recently locating to India across different sectors and regulatory frameworks since its inauguration in 2020.

- **Use of Real Estate.** Indian authorities have identified the integration of the proceeds of crime through the purchase of high value items such as real estate, in particular through 'benami ownership.'[14] The assessors focused on the extent that the real estate sector and other potential gatekeepers of real estate transactions are accurately identifying the beneficial owner of customers, understand the ML risks the sector faces, and are effectively applying more recent preventative measures.
- **Precious Metals and Stones (PMS).** The ease with which PMS can be used to move large amounts of funds without leaving an ownership trail combined with the size of the market in India means there are vulnerabilities associated with their use as a tool for ML/TF. The assessors explored the extent to which PMS are used as part of ML schemes including the interaction with dealers in PMS. The cross-border movement of PMS to the extent they are part of ML schemes was also considered.

### *Proliferation Financing*

- **Outreach to support implementation of TFS.** There is limited evidence available from public sources of particular sanctions evasion methodologies being used by sanctioned individuals and entities to evade sanctions in India. However, given India's large maritime borders, and more general typologies used to evade sanctions, assessors considered the outreach conducted by competent authorities with FIs, DNFBPs and other natural and legal persons involved in trade finance to support implementation of TFS.

### *Structural Issues*

- **Domestic cooperation and coordination.** The central agencies responsible for investigating and prosecuting ML and TF offences in India must work closely with other law enforcement authorities as well as State level authorities that are responsible for investigating predicate offences. Given the size and relative complexity of India's institutional system, and the varied threats India faces, including cross-State and cross-border threats, assessors analysed how India's different agencies work together.

57. These following issues were provisionally identified as lower-risk, and did not receive much attention in the course of the assessment:

- **Physical Casinos.** There are 22 licenced casinos operating in India, mostly in Goa. The level of activity in terms of participation of players, especially foreign entities as well as the stakes involved are minimal. The size of this sector is very small (excluding internet-based gaming which is growing quickly)[15].

[14] A Benami ownership structure is one where the real owner is other than the legal owner, concealing the identity of the true beneficiary. The term is considered synonymous with 'informal nominee.'

[15] The Public Gambling Act, 1867 provides for the basis of the gambling laws in India, differentiating between games of skill and games of chance. The PMLA considers as AML/CFT reporting entities as persons carrying out activities associated with playing games of chance for

- **Insurance and Pension Sectors.** A minimal number of cases have been investigated in India in which these sectors have been abused for ML/TF. India's 2022 NRA rates the risk as Low.
- **Financial inclusion products**. In light of the risk mitigating measures put in place in respect of financial inclusion products (Basic Savings Bank Deposit Accounts and Small Accounts), it was concluded that the overall vulnerability of these products is low in so far as they relate to ML/TF.
- **Small scale criminality, and rural vs urban population**. In light of the size of the country, assessors focused on large-scale criminality and laundering, and focused on centres where large-scale economic activity is taking place (i.e., cities) with less focus on rural activity and agricultural regions (and associated agricultural financing and insurance products).

## Materiality

### *Economy*

58. India's economy is the third largest in the world,[16] with a GDP of approximately USD 3.5 trillion. Output concentrated in India's cities.[17] [18] While India is considered a lower-middle-income country, it is one of the world's fastest growing economies growing by an average of 6-7% per year since 2000. Its model is often described as 'growth-led exports' rather than 'export-led growth' like many countries in the region, with its economy primarily driven by domestic consumption.[19]

59. India has drastically reduced extreme poverty over the last fifteen years.[20] Around 13% of the population currently live in extreme poverty, and just over 40% live in moderate poverty.[21] There is significant income inequality.[22]

60. India's economy encompasses a diverse range of outputs, from traditional village farming, modern agriculture, handicrafts, a wide range of modern industries and services. Services are the

cash or kind, and includes activities associated with casinos. The interpretation of what constitutes a game of skill or chance was most recently considered in 2015 by Supreme Court of India (MD Chamarbaugawala v. Union of India, AIR 1957 SC 628). The competence for regulating gambling falls to the States and only two States have permitted the operation of casinos (Goa and Sikkim). India has confirmed that neither State has accepted a licencing application from an online casino and therefore only physical casinos may operate in these two states (and across India).

16 On the basis of purchasing power parity.

17 World Economic Forum White Paper (2021). See www.weforum.org.

18 70% of GDP productivity is produced by residents of India's cities. IMF data mapper (2023). See www.imf.og.

19 See for example 'Trade Regimes and Export Strategies with Reference to South Asia', Ehtisham Ahmad published by the IMF.

20 Less than USD 2.15 per person per day, 2017 PPP, according to World Bank categorisation. Between 2011 and 2019, India is estimated to have halved the share of the population living in extreme poverty – below USD 2.15 per person per day (2017 PPP). World Bank Poverty and Inequality Portal and Macro Poverty Outlook, Spring 2023.

21 Moderate poverty is defined as less than USD 3.65 per person per day. World Bank Poverty and Inequality Portal and Macro Poverty Outlook, Spring 2024.

22 Estimates of 40% of the wealth created in India estimated to have been retained by 1% of the population, and 3% to the bottom 50% according to Oxfam India, calculation based on Credit Suisse data. See www.oxfamindia.org. The World Bank assesses India to have a high inequality based in differences in consumption. See www.worldbank.org/en/country/india/overview.

major source of economic growth, even though more than half of the workforce is employed in the agricultural sector. A large proportion of the workforce is employed informally, especially in the agriculture, construction and parts of the trade sector.[23]

61. In 2022, India's largest exports were refined petroleum (USD 49 billion), diamonds (USD 26.3 billion), pharmaceuticals (USD 19.2billion), jewellery (USD 10.7 billion) and rice (USD 10 billion). Primary destinations for exports were the United States (18.1%), the UAE (6.7%), China (5%) and Bangladesh (3.8%). India's largest imports in 2022 were of crude petroleum (USD 93.5 billion), gold (USD 58.4billion), coal briquettes (USD 28.4billion), diamonds (USD 26 billion) and petroleum gas (USD 21.9billion). Imports were primarily from China (15.4%), the UAE (7.4%) and the United States (7.1%).

62. India has no common borders with DPRK. It has diplomatic relations with DPRK and its exposure to DPRK is mainly related to trade, which is predominantly in agricultural products. However, trade is heavily restricted, has significantly declined since 2019, and is currently at an insignificant level, totalling less than approximately EUR 2 million in exports and imports respectively in 2021.[24]

63. There are no agreed upon estimates of the shadow economy in India. Estimates that have been made vary significantly, although generally identify a moderate to large shadow economy as a proportion of GDP.[25] Several factors imply the continued presence of a relatively large shadow economy despite the dramatic increase in the use of the formal financial system, including the amount of cash in circulation, the large informal workforce and analysis associated with the cash-based transactions in the NRA.[26]

### *Financial Sector*

64. India's financial sector is dominated by the banking sector, predominantly servicing domestic retail and commercial customers. Up until 2015, only universal banking licences were issued. Ten public sector banks were also consolidated into four in 2020,[27] resulting in 12 public sector banks and 21 private sector banks controlling significant market share.[28] Nevertheless, after 2015, new banking licences were granted resulting in a more diverse banking sector, with foreign banks, regional rural banks, urban cooperative banks, rural cooperative banks institutions, and 'niche' banks servicing low-income customers, the migrant labour force and the informal labour market all now operating in India.

---

[23] Informal employment is considered employment with no written contract, paid leave, health benefits or social security. The International Labour Organisation estimates the proportion to be more than 80% of the total workforce. See www.ilo.org.

[24] UN COMTRADE, India Ministry of External Affairs and the observatory for economic complexity.

[25] See for example IMF working paper Measuring Informal Economy in India: Indian Experience, S V Ramana Murthy. See also a study by the State Bank of India estimating that the informal economy in India shrunk from 52% of GDP in 2018 to less than 20% in 2020-21, based on estimates of the loss of economic output during the COVID-19 pandemic and assumptions linking the loss of output to the informal economy (available from www.sbi.co.in/documents, accessed February 2024).

[26] See IMF 2022 Article IV Consultation with India and NRA (2022).

[27] This significant consolidation exercise resulting in the amalgamation of Oriental Bank of Commerce and United Bank of India into Punjab National Bank; Syndicate Bank into Canara Bank; Andhra Bank and Corporation Bank into Union Bank of India, and Allahabad Bank into Indian Bank.

[28] Private sector banks increased their share of credit from 22% in June 2025 to 38% in June 2022. See www.rbi.org.in.

1

65. FDI in India has been consistently increasing over the last 10 years, more than doubling from USD 24 billion in 2012 to USD 50 billion in 2022, with a peak of USD 64 billion in 2021,[29] and a net inflow of 1.5% as of 2022. FDI into India has been helped by the relaxing of restrictions of foreign investment in some industries. India's capital markets have also almost doubled since 2018, with its stock market the seventh largest in the world by total market capitalisation, although characterised by a greater proportion of domestic rather than foreign investment.

66. India has also one of the world's largest and fasted growing fintech sectors,[30] and a growing number of VASPs. As a September 2023, India is ranked second-largest VA market in the world by raw estimated transaction volume.[31] India has also commenced a pilot for a Central Bank Digital Currency both for retail and wholesale use to complement its digital payment system, support the move towards a cash-less economy, and potentially help bring efficiencies in cross-border transactions.

67. India started creating structures to support an International Financial Centre in around 2011, with the aim of supporting the developing of financial markets in India and in the region, providing a variety of tax incentives for firms. The International Financial Services Centres Authority (IFSCA) was established under the IFSCA Act, 2019 as a unified regulator for regulating activities related to banking, capital market, insurance, pension funds and other notified financial products and financial services undertaken in IFSC.

### *Other key sectors*

68. Precious metals and stones play an important role in Indian tradition and culture and continue to be used a store of value for a large proportion of the population. India is currently the world's second largest consumer of gold, the largest importer, and the largest exporter of gold jewellery.[32] It also has one of the largest industries for polishing of diamonds and gems, and jewellery manufacture, with the gems and jewellery sector constituting approximately 7% of GDP (c. EUR 250 billion).

69. Companies can be set up in India by individuals (proposed director, manager or secretary) or by professionals (lawyer, accountant and company secretary). Accountants and Company Secretaries play an important role in company formation and administration due to the administrative process required to administer a company in India. Lawyers are involved in company formation but have not been given the ability to administer companies by the government, and there is a general prohibition on directly handling clients' funds.

70. India has a vibrant property market, consistent with its high economic growth over the preceding decades, currently valued at around EUR 200 billion. Real estate agents do not always play a role in real estate transactions, as there is no requirement to use their services. Real estate agents tend to be very large entities involved in investing capital on behalf of institutional investors of wealthy private individuals, or very small ones providing advice to individual customers.

---

29 The decrease from 2020 to 2021 is attributed to the impact on economic activity caused by the COVID-19 pandemic.

30 Industry reports indicate that the Indian FinTech sector received USD 25 billion in funding between July 2018 and July 2023, and is expected to grow at a rate of more than 35% annually reaching USD 190 billion in revenue by 2030. See State of the Fintech Union, Boston Consulting Group, available from www.bcg.com/publications/2023/india-state-of-the-fintech-union, accessed February 2024.

31 See Central & Southern Asia Crypto Adoption Trends and Analysis (chainalysis.com), accessed May 2024.

32 Gold imports were USD 46.14 billion in 2021-22. Smuggling In India Report 2021-22 by the Directorate of Revenue Intelligence.

71. India has a large non-profit sector, with more than three million NPOs, and 286 000 that have been assessed by India as falling within the FATF definition. The large number of NPOs active in India is primarily due to the size of India's population, with a decreasing but still significant number of people living in poverty as noted above (approximately 190 million in extreme poverty and 560 million in moderate poverty). Government funds and requirements on certain types of companies to spend a proportion of their profits on corporate social responsibility, has provided substantial funds to the sector every year (INR 263 trillion or EUR 2.9 billion in 2020-21).[33] There are strict rules that govern registration and the receipt of foreign donations.

### Structural Elements

72. India has the main structural elements that are required for an AML/CFT system to be put in place, including high-level commitment to address AML/CFT issues; political stability; stable institutions and rule of law.

73. India's high-level commitment to address AML/CFT issues is reflected through the measures it has taken over a number of years,[34] and at multi-lateral fora.[35]

74. India is the largest democracy in the world, achieving a smooth transfer of power following each election since its independence.[36] India ranks moderately accordingly to the World Justice Project Rule of Law Index,[37] and above average when compared to its peers from middle income countries.[38]

75. The Constitution of India provides for a directive to separate the judiciary from the executive, which is implemented through the Code of Criminal Procedure (1973) and case law.[39] There are some concerns identified relating to the length of time it takes to conclude trials in IO.7 and IO.9.

### Background and Other Contextual Factors

76. India has assessed the threats associated with corruption and bribery as medium-high, with the finding supported by external sources suggesting that there is corruption in the judiciary, law

---

33 See www.csr.gov.in/content/csr/global/master/home/home.html. Access February 2024.

34 For example, the While Paper on Black Money (2012), which ultimately led to a number of policy interventions including the withdrawal of higher denomination bank notes; and through restrictions on transactions by *benamidars* (including informal nominees) to address benami property ownership. See Chapter 2.

35 For example, advocating for greater prioritisation of asset recovery as part of its G20 Presidencies in 2011 and in 2022. See Chapter 3,

36 In 2022, India's scored slightly above the global average in the World Bank's Voice and Accountability indicator, although its score has been marginally decreasing year-by-year since 2016; and scored very close to the global average for the World Bank Rule of Law Index with marginal improvements since 2020.

37 Seventy-seven out of 140 countries as of 2022, with more positive scores for underlying indicators on constraints on government powers, openness of government and order and security; and less positive scores for absence of corruption, civil and criminal justice.

38 15th out of 38

39 Article 50 of the Constitution of India. The Kesavananda Bharati case (year 1973/4SSC/225) laying the basic structure of Indian Constitution is a landmark judgement which established the independence of Indian judiciary.

enforcement, public services and procurement activities.[40] A large number of challenges in implementation of the UNCAC were identified in its review adopted in 2020, including the need for India to criminalise transnational bribery and bribery in the private sector, enhance whistle-blower protection, strengthen domestic cooperation and strengthen the independence of law enforcement authorities investigating and prosecuting corruption and money laundering offences.

77. Tackling corruption is a stated priority of the government of India through its 'Zero Tolerance against Corruption' policy. During the onsite, India provided the assessors with information on the institutional structures that have been put in place to help identify cases of bribery in the public service, specifically the role played by the Central Vigilance Commission (CVC), an autonomous body responsible for tackling governmental corruption. Other recent measures include expansion of the Bribery Act (2018) to include direct transfer of welfare benefits, the implementation of e-tendering for public procurement, and amendments to the rules providing timelines for disciplinary proceedings for civil servants.

78. Assessors also note the lack of requirements in relation to domestic Politically Exposed Persons (PEPs) (see Rec.12), which would assist the private sector in identifying such customers and in undertaking the additional measures necessary to mitigate the risk that they would represent.

79. India was generally considered a centrally planned, closed economy following its independence in 1947. Major reforms have been introduced since the early 1990s including liberalisation of the economy, reducing regulation and helping integrate the Indian economy and financial system into the global economy and financial system. These reforms continue. As of 2019, India ranked 63 in the World Bank's ease of doing business index in 2021 when data for some countries was collected by World Bank.[41] Capital controls have also been gradually reduced since the early 1990s. Currently there are no restrictions on residents remitting up to USD 250 000 per financial year for any permitted current or capital account transaction (or a combination) through authorised channels,[42] or on businesses conducting payments or receiving receipts for goods or services. Overall, while the Indian economy is significantly more liberal than it was in the 1990s, a large number administrative requirements remain on individuals and firms in India, and in some examples these act as mitigating measures, reducing vulnerabilities for ML and TF. These are referenced in more detailed in relevant sections of the main body of the report.

---

40 See the Transparency International's Corruption Perception Index, Transparency International India Corruption Survey (2019) and the World Bank 'Doing Business' Survey or the World Economic Forum Global Competitiveness Report.

41 Rank of 1 represents the country with scoping the highest in the World Bank's Index. India's Gini Index score according to the 2019 survey was 35.7. The score is based on a set of 41 indicators that reflect regulatory best practice that help facilitate business, for example how quickly a company can be setup or how efficiently property can be transferred. A score of 100 correlates with the highest possible ease of doing business score (i.e., a regulatory framework that helps facilitate business), and a score of 0 the lowest. The data collection exercise was discontinued by the World Bank in 2021 and 2019 is the last remaining year for which data is publicly available. India scored 34.2 in 2021 when data for some countries was collected.

42 That is, residents of India are permitted to buy or sell foreign currencies or transaction in foreign currencies up to the threshold of USD 250 000. The set of restrictions include remittance where transactions cannot take place includes income from lottery winnings and other forms of gambling, income from racing or any other hobby, and banned items. Authorised channel means a financial institution licenced to carry out foreign exchange transactions. See R.14. Some specific restrictions do apply, such as remittances directly or indirectly made to countries identified by the FATF as non-cooperative. For information see www.rbi.org.in 'liberalised remittance scheme' updated 6 April 2023 (accessed February 2024), which is based on provisions on the Foreign Exchange Management Act 1999.

80. India was significantly affected by the COVID-19 pandemic that occurred from 2020 to 2023. This had an impact on the supervisory cycle due to limits on the level of physical interaction that could take place. This also impacted the broader risk environment as online scam and extortion cases against Indian nationals grew impacting the fintech, banking and securities sector as discussed in the 2022 NRA. While the government made attempts to enable government business to continue through virtual communication to the extent practical and possible, it also affected the efficiency of the government and judicial system similar to other countries. Further information on the impact of the COVID-19 pandemic has not been provided, although this is considered in relevant sections of this report.

### *AML/CFT strategy*

81. India adopted a National Strategy on AML/CFT in 2023, drawing from the NRA (2022). The National Strategy includes two tracks. The first provides six sets of action points to respond to some of the specific findings in the NRA. These are devoting more resources to the investigation of high-risk predicate threats; developing the supervisory regime of some of the sectors that have more recently been brought into the scope of the AML/CFT framework (real estate agents, company secretaries and accountants); deepening the framework for beneficial ownership; and identifying and assessing risks associated with NPOs. The second sets out seven broader themes covering some the key elements of an AML/CFT regime to be improved that includes the detection and investigation of ML cases, asset recovery, and domestic cooperation and coordination. Each theme has several short and longer-term actions under it.

82. Before the National Strategy was adopted in 2023, AML/CFT policies and objectives were set out in an ad hoc manner, some of which were in response to the last FATF mutual evaluation in 2010, to a 2012 White Paper on Black Money, or other distinct policy measures for example responses to cybercrime.

83. Policies have been put in place in India to encourage use of the formal financial system. JAM or Jan Dhan, Aadhaar, and Mobile refers to a series of policy interventions in 2014 that expanded affordable access to bank accounts and other financial services, introduced a biometric identification system, the largest in the world, and supported the development of a digital mobile payment system. Together with other policy interventions, such as the development of digital payment infrastructure, there has been a rapid increase in the digital transaction volumes from 20.7 billion transactions in 2017-18 to 134.6 billion in 2022-23.[43] The Goods and Services Tax, introduced in 2017, has also had an impact on bringing individuals and businesses into the formal economy, as it unified VAT, previously implemented independently by States, and utilises the electronic transmission of invoicing.[44]

### *Legal & institutional framework*

84. The overarching legal framework for AML and CFT in India is set out in the Prevention of Money-Laundering Act, 2002 ('PMLA') and the Unlawful Activities (Prevention) Act, 1967 ('UAPA') respectively. Legislative Acts concerning asset recovery are also found in the Fugitive Economic Offenders Act ('FEOA'), the Prevention of Corruption Act ('PCA'), and the Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act ('SAFEMA'), the Customs Act, the Narcotics Drugs and Psychotropic Substances (NDPS) Act and the Arms Act. The UAPA and the Weapons of Mass Destruction and their Delivery Systems Act provide the legal basis for the implementation of targeted financial sanctions. The Criminal Procedure Code sets out the underlying basis for and requirements on the conduct of law enforcement authorities.

[43] See www.pib.gov.in [accessed February 2024]

[44] Required for all transactions above INR 50 000 (EUR 562).

1

85. The Government has been subject to supreme court challenges to the legal framework for AML that have affected its operation. Since 2014, there have been several challenges to the constitutionality of elements of the PMLA. In July 2022, the Supreme Court found the PMLA to be constitutionally valid. This meant that there was disruption to the progress of prosecution of cases under the PMLA during the period 2014-2022. The effects on India's AML/CFT framework are identified where relevant throughout the report.

86. The below lists the key authorities responsible in India for the AML/CFT framework listed by the ministries with a policy responsibility; the coordination mechanisms, key national authorities for ML and TF; national authorities responsible for the predominant predicate offences; and relevant State authorities.

87. The following four ministries are responsible for the AML/CFT framework in India.

- **The Ministry of Finance (MoF):** The MoF is responsible for the AML framework in India, with oversight of the PMLA. The MoF is the parent ministry for the following LEAs enforcing the PMLA: 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 Department for Revenue at the MoF is responsible for the framework for targeted financial sanctions for proliferation financing.
- **The Ministry of Home Affairs (MHA):** The MHA is responsible for internal security in India including combatting terrorism and terrorist financing, with oversight of the UAPA. The MHA is the parent ministry for the following LEAs enforcing the UAPA: the National Investigation Agency, the Narcotics Control Bureau, and the Intelligence Bureau. The MHA is also responsible for the National Investigation Agency Act, 2008 (NIA Act) that constitutes the NIA, and is the central authority for Mutual Legal Assistance in criminal matters.
- **The Ministry of Corporate Affairs (MCA):** The MCA is responsible for administration of corporate entities in India, with oversight of the Companies Act, 2013 and other associated Acts and rules and regulations, including the Partnership Act; the Societies Registration Act; Limited Liability Partnership Act, 2008 and the Competition Act, 2002. The MCA also oversees three professional bodies that conduct supervision, namely, the ICAI, the ICSI and ICWAI. See below.
- **The Ministry of External Affairs (MEA).** The MEA is responsible for processing extradition requests in all criminal matters, including those relating to ML and TF.

88. The following mechanisms have been put in place to support domestic coordination and cooperation in India.

- **The Economic Intelligence Council (EIC):** The EIC is mandated to identify and discuss trends in economic offences (i.e., money laundering and predicate offences with a financial competent such as tax evasion or bank fraud), strategies on intelligence sharing, and oversee co-ordination. The EIC is chaired by the Minister of Finance, with representation from senior representatives from Ministries and intelligence agencies, the Governor of the RBI and the Chairman of the SEBI. Its mandate includes formulating a work-plan of the agencies. It is responsible for reviewing important cases involving multiple agencies and approving the modalities required to support interagency cooperation, examining emerging methods and trends and putting in place measures to respond to them.

- **The Central Economic Intelligence Bureau (CEIB):** The CEIB provides a link between the EIC and the operations of enforcement agencies. Under the CEIB, Regional Economic Intelligence Councils (REICs) have been set up across the country to help co-ordinate the work among various enforcement and investigating agencies dealing with economic offences (see above).
- **The Inter-Ministerial Co-ordination Committee on Combating Financing of Terrorism and Prevention of Money Laundering (IMCC):** The IMCC is responsible for policy and operational co-ordination at director level across all relevant competent authorities, including LEAs, supervisors and the FIU. The IMCC is chaired by the Secretary of the Department of Revenue within the Ministry of Finance.

89. The following competent authorities are the key operational agencies for AML/CFT in India, with nation-wide responsibilities for ML, across predicate offences or for TF:

- **The Financial Intelligence Unit of India (FIU-IND):** FIU-IND was set up by the Government of India in 2004 and is part of the MoF. In addition to its role as the central national agency for receiving, processing, analysing and disseminating information relating to suspect financial transactions, as well as large cash transactions, FIU-IND supports coordination via role developing and sharing financial intelligence both domestically and internationally with other FIUs, and plays a role in supervision of regulated entities (see below).
- **The Directorate of Enforcement (ED):** The ED is responsible for the investigation and prosecution of money laundering offences and confiscation of the proceeds of crime under the PMLA across India, with field offices in various States and Regions in the country. The ED is also responsible for enforcing provisions of FEMA, which includes powers to prevent the illegal operation of Hawaladars and associated cross-border transactions.
- **The National Investigation Agency (NIA):** The NIA is responsible for the investigation and prosecution of offences under the UAPA, including TF offences. The NIA has concurrent jurisdiction with States. The Courts may *suo moto* assign a case to the NIA.

90. The following competent authorities are the key operational agencies for AML/CFT in India, with mandates focusing on major predicate crimes for ML in India:

- **The Narcotics Control Bureau (NCB):** The NCB is an apex co-ordinating agency, meaning it coordinates the work of other law enforcement authorities (Drug Law Enforcement Agencies or DLEAs)[45] that are responsible for prosecuting offences relating to the trafficking or possession of illegal drugs and psychotropic substances. The NCB also has powers to investigate and charge offences under India's Narcotic Drugs and Psychotropic Substances (NDPS) Act, and trace and freeze illegally acquired property associated with offences under the NDPS Act.
- **The Central Bureau of Investigation (CBI):** The CBI is responsible for enforcing offences of corruption, committed by officials of the Central Government and

[45] An example of such a 'nodal agency' that the NCB may coordinate is the Central Bureau of Narcotics CBN) that supervisors and monitors licit cultivation of opium poppy production in India, issues licences for the manufacture and export or import of synthetic narcotics and fulfils India's obligations under the UN Drug Control Conventions and at the International Narcotics Control Board.

associated bodies or organisations across India. This includes the investigation and prosecution of these offences and mutual legal assistance associated with cases and the extradition of offenders.

- **The Serious Frauds Investigation Office (SFIO):** The SFIO is responsible for investigating corporate frauds of a serious and complex nature across India.
- **The Central Board of Direct Taxes (CBDT):** The CBDT is a statutory authority, part of the Income Tax Department (ITD), that is responsible for administering all matters relating to direct taxes, including tax evasion, across India. The ITD has a dedicated investigation department with offices across India. The ITD also has a department responsible for the registration and compliance of NPOs with their obligations under the Income Tax Act, the Commissionerate of Exemptions.
- **The Central Board of Indirect Taxes (CBIC):** The CBIC is a statutory authority and part of the Department of Revenue, MoF. The CBIC is responsible for the formulation of policy concerning the levy and collection of customs and excise tax revenue. It is also responsible for the administration of Goods and Services Tax. It is in charge of the prevention and investigation of smuggling offences and is responsible for the administration and enforcement of the declaration system regarding the physical cross-border transportation of currency or bearer negotiable instruments (BNI).
- **The Directorate of Revenue intelligence (DRI):** The DRI is part of the CBIC and is responsible for the collection of intelligence, analysis, and dissemination of intelligence associated with violations of customs laws, and has concurrent jurisdiction over anti-narcotics laws with other DLEAs as part of the CBIC. It is also the agency responsible for India at the World Customs Organisation (WCO), the Regional Intelligence Liaison Office (RILO), INTERPOL[46] and foreign Customs Administrations.
- **Bureau of Immigration (BOI):** There are 86 immigration checkpoints allowing entry in and exit from India. 37 are controlled by the BOI while the remaining 49 are controlled by the State Governments.

91. The following competent authority plays an important role at State level across relevant crime types:

- **The State Police:** Under the Constitution of India, 'Police' and 'Public Order' are State subjects. Every State and Union Territory has its own police force. The State Police has concurrent jurisdiction with the NIA in the investigation of terrorism and TF cases. The State Police also investigate and prosecute offenders for other offences, a number of which constitute predicate offences under the PMLA. Economic Offence Wings (EoW) are specialised units within State Police Departments that are tasked primarily with investigating, but also prosecuting economic crimes. EoWs tend to focus on more complex white-collar crimes that typically involve large sums of money, multiple parties and more intricate schemes. Counter terrorism units (Anti-terrorism Squads) have been set up to investigate terrorism and TF cases within States.

92. The following coordination mechanism plays an important role across authorities:

[46] DRI is the Customs agency identified as INTERPOL Liaison Office for Mutual Legal Assistance.

- **Multi-Agency Centre/Subsidiary Multi-Agency Centre (MAC/SMAC)**: The MAC at the central level (supported by SMACs at the State level) is a coordination body for sharing intelligence inputs, coordination with representatives from state governments, numerous agencies, and ministries on national security matters, across authorities. There are sub-groups focused on key aspects of ML and TF and participating authorities depend on the focus of the sub-group. The work of the MAC/SMAC coordination mechanism is referenced in different parts of the MER.

### *Financial sector, DNFBPs and VASPs*

93. India is not an international financial centre, although it has put in place structures to help establishing one in the future through the IFSC (see below). The banking sector plays an important role in India's financial sector, with banking assets representing 92.3% of GDP.[47] India does not have any Global Systemically Important Banks (G-SIBs) headquartered in the country.

94. The IFSC has 297 operating entities including 23 banking units (seven of which are foreign G-SIBs), six market infrastructure institutions, 133 capital market intermediates, 36 funds management entities, 24 insurance and reinsurance entities, and intermediary offices and 43 DNFBPs. They represent a relatively small proportion of India's financial services sector.[48]

95. India's approach to VASPs has developed over time. In 2013, RBI issued a circular cautioning users of the risks of virtual assets, and in 2018 issued a prohibition on RBI regulated entities (banks, NFBCs and payment service providers) from dealing in virtual assets or facilitating any person or entity settling transactions in virtual assets. Draft legislation published for consultation in 2019 seeking to ban virtual assets did not proceed to parliament due to the response from stakeholders. In 2020, the Supreme Court quashed the RBI circular issued in 2018, concluding it was disproportionate. In July 2022, tax at source of 1% of any payment or transfer of virtual assets was introduced and since March 2023 virtual asset service providers are subject to registration and AML/CFT obligations.

96. The size of the DNFBP sector in India is relatively large compared to many countries (around 14% of GDP), largely due to the demand for and services relating to precious metals and stones (7% of GDP) and real estate (5% of GDP).

97. India is not a company formation centre. Lawyers, chartered cost and works accountants, and company secretaries can assist forming companies as per company law requirements. Due to administrative restrictions and scope of advocates' activities in India, lawyers (advocates) do not engage in regular company filings after company formation or the business of managing legal entities. Only advocates registered with a State Bar association can provide legal services in India. Lawyers and accountants do not regularly deal with client funds, although a small percentage of accounting firms or professionals reported conducting financial transactions for or on behalf of clients as part of their regular business activities. Most corporate services are provided by accountants and company secretaries, even if other TCSPs also operate in the market.[49]

---

47. Scheduled Commercial Banks only. As on 31 March 2022. See 2023 Article IV Submission of India to the IMF.

48 The total asset of all banks in IFSC is about USD 37 billion on April 30, 2023. The turnover of stock exchanges in the IFSC during FY 2022-23 was USD 447 Billion.48 As on March 31, 2023, the cumulative listing of all the debt securities on the recognised stock exchanges in the IFSC was USD 50.6 billion. FMEs have collectively raised commitments of approx. USD 13 Billion across 50 schemes as on March 31, 2023.

49 India estimates that 85% TCSP services are provided by accountants and company secretaries, whilst the 15% remaining is dealt with by other TCSP professionals (SRA "ML/TF risk profile of DNFBPs – Accountants, Lawyers and TCSPs", dated 28 August 2022).

1

98. While the market for precious metals and stones is one the largest in the world, a prohibition on the receipt of cash over INR 200 000 (EUR 2 222) under tax law limits the extent that R.22 and R.23 capture dealers' activities. Nevertheless, as part of Goods and Services Tax (GST) requirements, DPMS dealers must be registered, and their details verified by GST authorities. Import and export must be registered with Director General of Foreign Trade (DGFT), which issues a unique Import Export Code (IEC). The Gems and Jewellery Export Promotion Council (GJEPC) as the apex body for the gems and jewellery industry that are involved in import or export, is also active in preventing malpractices. In March 2023, the Ministry of Consumer Affairs, Food and Public Distribution issued an order to prohibit the sale, display or offer to sell any gold jewellery or gold artefacts that are not hallmarked in accordance with the specified standards by the Bureau of Indian Standards. The purpose of this initiative is to protect the public against adulteration but this also helps to increase the visibility of the legitimate supply chain and illicit mixing of gold jewellery. However, there is insufficient information as to the extent to which this prohibition is enforced across the DPMS sector across the country or how this impacted risk understanding of the sector in the NRA. All rough diamond imports are controlled by the Kimberly Process Certification Scheme since 2004 and thus require a KP certificate.

99. The population of firms and size of assets held (for financial institutions) is described in the following table, which also includes the number of entities in each sector registered with FIU-IND as reporting entities:

### Table 1.1 Overview of India's Financial Sector (2023)

| | Number of entities registered with supervisors (as at Mar 2023) | Assets Held [INR trillion] | Assets Held EUR (Billion) | Reporting Entities registered with FIU-IND (as at Nov 2023) |
|---|---|---|---|---|
| **Banking Sector (RBI)** | **2 027** | **272.46** | **3 044.1** | **2 322** |
| Public Sector Banks (excluding SBI) | 11 | 85.6 | 957 | |
| State Bank of India | 1 | 56.8 | 634 | |
| Private Sector Banks | 21 | 85 | 950 | |
| Foreign Banks | 43 | 15.8 | 176 | |
| Small Finance Banks | 12 | 2.7 | 30 | |
| Payment Banks | 6 | 0.24 | 3 | |
| Local area banks | 2 | 0.02 | 0.1 | |
| Tier 1 Urban Cooperative Banks (UCBs)[50] | 898 | 0.9 | 10 | |
| Tier 2 UCBs | 520 | 2 | 23 | |
| Tier 3 UCBs | 78 | 2.4 | 26 | |
| Tier 4 UCBs | 6 | 1.5 | 17 | |
| State Cooperative Banks* | 34 | 4.6 | 51 | |
| District Central Cooperative Banks | 352 | 7.0 | 78 | |
| Regional Rural Banks[51]* | 43 | 7.9 | 89 | |

[50] UCBs have been categorised into following four tiers for regulatory purposes:
- *Tier 1* -All *unit* UCBs and salary earner's UCBs (irrespective of deposit size), and all other UCBs having deposits up to INR 1 billion (EUR 11 million);
- *Tier 2* - UCBs with deposits more than INR 1 billion (EUR 11 million) to INR 10 billion (EUR 111 million);
- *Tier 3* - UCBs with deposits more than INR 10 billion (EUR 111 million); INR 100 billion (EUR 1.1 billion); and
- *Tier 4* - *UCBs* with deposits more than INR 100 billion (EUR 1.1 billion).

[51] Regulated and licensed by RBI but supervised, including for AML/CFT, by NABARD.

| | Number of entities registered with supervisors (as at Mar 2023) | Assets Held [INR trillion] | Assets Held EUR (Billion) | Reporting Entities registered with FIU-IND (as at Nov 2023) |
|---|---|---|---|---|
| | | | | |
| **Non-Banking Financial Sector (RBI)** | **9 568** | **72.4** | **808** | **11 882** |
| Type of non-bank financial company (NBFC) – base layer[52] | 9 113 | 3.6 | 40 | |
| NBFC – middle layer | 319 | 38.8 | 433 | |
| NBFC – upper layer | 11 | 12.8 | 143 | |
| NBFC – top layer | 0 | | | |
| Asset Reconstruction Companies | 28 | 0.3 | 3 | |
| Housing Finance Companies[53] | 97 | 16.9 | 189 | |
| | | | | |
| **Payment System Operators** | 67 | 5.37 | 60.01 | **103** |
| | | | | |
| **Foreign exchange** | **1 857** | **0.6074** | **6.8** | **1 912** |
| FFMC | 1 814 | 0.1974 | 2.2 | |
| Non-bank Authorised Dealers Cat-II | 43 | 0.41 | 4.6 | |
| | | | | |
| **Capital Markets (SEBI)** | **25 598** | | | **4 420** |
| Stock Exchanges | 5 | 258.20 | 2 881.44 | |
| Depository institutions | 2 | 341.90 | 3 815.53 | |
| Capital Market Intermediaries (assets under custody) | **25 591** | 172.22 | 1 910 | |
| | | | | |
| **Insurance (IRDAI)** | **69** | **60.03** | **670.06** | **329** |
| Life Insurers | 25 | 54.63 | 609.70 | |
| General Insurers | 27 | 4.03 | 44.99 | |
| Standalone Health Insurers | 5 | 0.26 | 2.93 | |
| Reinsurers (including Foreign Reinsurance Branches) | 12 | 1.11 | 12.44 | |
| Insurance brokers | 616 | N/A | N/A | |
| | | | | |

[52] NBFCs have been categorised as under:
- *Base Layer*: (a) non-deposit taking NBFCs with assets below INR 10 billion (EUR 111 million); and (b) NBFCs undertaking the following activities- (i) NBFC-Peer to Peer *Lending* Platform (NBFC-P2P), (ii) NBFC-Account Aggregator, (iii) Non-Operative Financial Holding Company and (iv) NBFCs not availing public funds and not having any customer interface.
- *Middle Layer*: (a) all deposit taking NBFCs, irrespective of asset size, (b) non-deposit taking NBFCs with asset size of INR 10 billion (EUR 111 million) and above and (c) NBFCs undertaking the following activities (i) Standalone Primary Dealers, (ii) Infrastructure Debt Fund - Non-Banking Financial Companies, (iii) Core Investment Companies, (iv) Housing Finance Companies and (v) Infrastructure Finance Companies.
- *Upper Layer*: NBFCs which are specifically identified by RBI as warranting enhanced regulatory *requirement* based on a set of parameters and scoring methodology. The top ten eligible NBFCs in terms of their asset size always reside in the upper layer, irrespective of any other factor.
- *Top Layer*: this layer will ideally remain empty. it can be populated if the RBI is of the opinion that there is a substantial increase in the potential systemic risk from specific NBFCs in the Upper Layer. Such NBFCs shall move to the Top Layer from the Upper Layer.

[53] Regulated by RBI but supervised by the National Housing Bank (NHB).

| | Number of entities registered with supervisors (as at Mar 2023) | Assets Held [INR trillion] | Assets Held EUR (Billion) | Reporting Entities registered with FIU-IND (as at Nov 2023) |
|---|---|---|---|---|
| **Pensions (PFRDA)** | **396** | **1.88311** | **21.007** | **64** |
| NPS – Citizen Model and Corporate | 97 | 1.56173 | 17.423 | |
| NPS Lite | 42 | 0.04915 | 0.548 | |
| Atal Pension Yojana | 229 | 0.27223 | 3.036 | |
| | | | | |
| **VASPs** (as on 26 Mar 2024) | **28** | **0.207** | **2.3** | **28** |

Source: RBI, SEBI, IRDAI, PFRDA, IFSCA and FIU-IND.

100. There is a mismatch in the records of the number of entities maintained by the supervisors and those registered with FIU-IND as reporting entities. This is partially explained by the different dates those statistics were extracted, and as FIU-IND may contain some historical data (e.g., banks have since been merged or closed businesses). There is a significant mismatch in the number of capital market entities registered with SEBI and with FIU-IND. This difference appears to be due to the fact that some intermediaries have multiple registrations with SEBI depending on the number of registered activities and that foreign portfolio investors, who are deemed to be intermediaries for regulatory purposes, are not reporting entities registered with FIU-IND. Therefore, it was not possible to quantify the universe of regulated entities that are required to register with FIU-IND but have not yet done so.

### Table 1.2. Overview of India's DNFBP Sectors (2023)

| | Total number | Considered AML/CFT reporting entities (R.22) | Number of REs registered with FIU-IND (Nov 2023) |
|---|---|---|---|
| Real Estate Agents | 82 75554 | 700255 | 144 |
| Dealers in Precious Metals and Stones | est.168 58556 | Nil | 47 |
| Lawyers | est. 2 300 000 | Nil | Nil |
| Accountants & company secretaries | 169 673 | 169 673 | 12057 |
| Members of Institute of Chartered Accountants of India (ICAI) | 158 119 | 158 119 | |
| Members of Institute of Cost Accountant of India (ICMAI) | 4 414 | 4 414 | |
| Members of Institute of Companies Secretaries of India (ICSI) | 11 554 | 11 554 | |
| Casinos | 23 | | 22 |
| Onshore Casinos | 17 | | |
| Offshore Casinos | 6 | | |
| Online casinos | Nil | Nil | Nil |

54 SRA "ML/TF risk profile of DNFBPs – Accountants, Lawyers and TCSPs", dated 28 August 2022.

55 Real estate agents with a minimum annual turnover of INR 2 million (EUR 22 000) are AML/CFT obligated entities in India, as per Notification G.S.R. 798(E) dated 28.12.2020.

56 Number of DPMS registered with the Bureau of Indian Standards, in connection with the hallmarking of jewellery. It does not include PMS refineries, gold bullion traders, goldsmiths etc.

57 India estimates that only 120 accountant professionals/ accounting firms perform conduct financial transactions for or on behalf of their clients within the meaning of Recommendation 23.1. In addition to the professionals ICAI, ICMAI and ICSI are also registered as reporting entities with FIU-IND to submit STRs on behalf of their members.

| | Total number | Considered AML/CFT reporting entities (R.22) | Number of REs registered with FIU-IND (Nov 2023) |
|---|---|---|---|
| TCSPs58 | 36 | 36 | 36 |

Source: Regulators

101. The difference in the number of DNFBPs registered with supervisors and those registered with FIU-IND relates to the fact that DNFBPs are not required to register with FIU-IND prior to submitting STRs (i.e., registration can be performed quickly when a STR is being submitted). In addition, differences are the result of accountants and company secretaries being able to submit STRs through their professional bodies which are also registered in FIU-IND's system.

102. The assessors weighted the sectors based on their relative importance, given their respective materiality and level of ML/TF risks. The assessors used these rankings to inform their conclusions throughout this report, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report but is most evident in Chapter 6 on IO.3 and Chapter 5 on IO.4.

103. The sector considered most important and weighted most heavily:

- **The Banking Sector** is by far the biggest sector in terms of share of financial sector assets in India. The banking sector also represents one of the channels that enables remittance to be sent to or from India and to enable investments in the securities market. The NRA identified this sector as being exploited by criminals to commit predicate offences and place or layer proceeds in the financial system for two of the most significant threats - bank fraud and cyber-enabled fraud. In addition, several of the other major threats identified in the NRA have a nexus with the banking sector, including bank accounts held by shell companies, accounts of legal entities being misused to commit trade-based money laundering, or the deposit or withdrawal of cash. Most MVTS business in India is conducted via banks.

104. Sectors considered important and weighted heavily:

- **Other financial institutions (OFIs)**: OFIs in India include a variety of institutions from payment system operators (PSO) facilitating digital and other transactions, non-banking financial companies (NBFC) that are deposit-taking and hold significant assets, authorised dealers in foreign exchange and money changers.
- **MVTS** is the one of the main mechanisms for transferring funds into and out of India. MVTS is mainly provided by NBFCs, although PSOs and the Department of Posts (DoP) also provide MVTS domestically. Also, under the Money Transfer Services Scheme (MTSS) for inwards remittances, banks, authorised dealers in foreign exchange (Category-I or Category-II including NBFCs), FFMCs, Department of Post) act as Indian agents of foreign principals. The TF NRA identified that the MTSS poses the highest threat across different theatres, after cash-couriers and hawala. MVTS including hawala are also identified as channels used to launder proceeds of other crimes. The nature of the services provided also gives rise to vulnerabilities, due to the frequency of occasional customers and therefore more limited data to base CDD, high number of cash payments, and the nature of agent-business relationship characteristic of the sector in India.

[58] This refers to individuals or legal entities that TCSP services in India and are not covered by another PMLA notification (e.g., TCSPs that are not company secretaries or intermediaries in the securities sector).

- **NBFCs** cover a range of services, with a small number of firms (10) accounting for 44% of total asset size (around INR 55 trillion or EUR 610 billion), of which the most significant firms are three infrastructure finance companies (59%) followed by six investment and credit companies (35%). While NBFCs play a more limited role in provision of credit in India compared to commercial banks, and the ML and TF threats associated with the sector has not been clearly established in the NRA, the sector of NBFCs cover around ten thousand entities, with assets broadly equivalent to 2/3 of assets of private banks. The remaining **OFIs** are involved in wide variety of financial activities, including infrastructure debt, micro finance, factoring, mortgage guarantees, housing finance and asset reconstruction companies.
- **VASPs:** The NRA identifies a wide range of risks associated with the misuse of VAs, including anonymity, weaknesses in compliance in the sector in India and globally, use of nominees, prevalence of 'pull rug' scams, emergence of ransomware and laundering through virtual assets. Cases of the VAs being used to transfer funds linked to terrorism have also been increasing. Like many other countries, India's framework for AML/CFT has recently been put in place. India's is relatively small in terms of number of reporting entities,[59] although there are materially significant VASPs operating in the country with large user bases [60] and conducting material trading volumes. [61] India ranks the second VA market in the world in terms of raw transaction volume.
- **Real Estate Agents:** The size of the real estate sector in aggregate and as a share of GDP has been growing rapidly. Similarly, foreign investment in the real estate market has also been growing quickly, primarily in commercial property, although remains a small proportion of the value of the real estate market (around 10%). The threats associated with real estate being used as a store of value in India appear to be significant, with the threat identified in the NRA as 'high' with a large number of cases relative to the size of the sector. The main threats identified are cash transactions and benami (nominee) ownership. During the on-site, the risk of under/over valuing property was also discussed although publication of property values may have limited this. A mitigating factor for the sector that has reduced the weighting is the fact that there is no requirement to use a real estate agent, although statistics are not available on the proportion of sales that take place through via a real estate agent.
- **Professional gatekeepers** (Accountants and Trust and Company Service Providers, including Company Secretaries): The vulnerability of legal persons in relation to their misuse as part of trade-based money laundering schemes, and use of shell companies to launder proceeds are both identified as significant in the Sectoral Risk Assessment of legal persons and arrangements and the NRA. Chartered Accountants, Cost and Works Accountants and Company Secretaries can perform company formation and administration services, although some services (e.g. provision of office address and domiciliation service) are restricted due to company law provisions in India on verification of business addresses, introduced to discourage the registration of multiple (shell) companies with a

[59] Twenty-eight registered VASPs as of November 2023.
[60] More than 1 million users.
[61] With trading volume of more than 0.25% of global trading volume.

single address[62]. TCSPs that are not company secretaries or accountants cannot act as company formation agents but in practice provide a number of corporate services, such as compliance work related to the management of companies.

105. Sectors considered neutral:

- **Securities Sector:** The Securities Sector in India is growing but is relatively modest in size compared to the size of the economy. The portfolio of relatively straightforward products, and the measures put in place to record customers and details of transactions help mitigate the risks. However, some threats do transpire, in particular as a result of the predicate offences of insider trading and market manipulation, with the quantum of proceeds laundered in cases often large.

106. Sectors considered less important and weighted to a limited extent:

- **Lawyers:** lawyers in India carry out activities covered by the FATF Standards only to a limited extent. Similar to accountants and company secretaries, they can provide a declaration for the purposes of company formation, but their involvement in other aspects of a company's management is limited due to restrictions applicable to the legal profession in India. Lawyers do not manage client's assets, including bank accounts, and do not provide business address or other administration services. Lawyer's involvement in real estate transactions are limited to drafting contracts and deeds and providing legal advice. There are no other type of legal professionals in India since only advocates can practice law.
- **Casinos**: Games of chance are prohibited in India, although they are permissible if an exemption is granted at State level. There are two States that have made an exemption to allow for physical casinos, both onshore and offshore. However, these are very small in number (see table above). There is limited evidence that they have been misused in India to launder proceeds.
- **Life Insurance and Pension Sectors**: Despite the size of the respective sectors, very few cases have been identified in the NRA, while it does not appear that there are any specific vulnerabilities in the products and services offered by firms in India.

107. A key DNFBP sector not considered in the categories above is the **DPMS sector**. This is because India has implemented a prohibition on cash receipts above INR 200 000 (EUR 2 222) under the Income Tax Act. Therefore, there are mitigating measures given that the FATF requires DPMS to be captured with the AML/CFT framework under R.22 and R.23 only when they engage in a cash transaction equal to or above the designated threshold. As a result, these recommendations have been considered not applicable for DPMS in the TC Annex. India has nevertheless recently introduced an AML/CFT framework for DPMS given that income tax policy may change in future independently of the AML/CFT framework, and due to the materiality of the sector. In addition, there is evidence that there are challenges implementing prohibition in a sector that includes more than 175 000 DPMS.[63]

---

62 SRA "ML/TF risk profile of DNFBPs – Accountants, Lawyers and TCSPs", dated 28 August 202.

63 There are not exact figures available on the number of DPMS as defined by the FATF Standards in India. There are 168 585 DPMS registered with the Bureau of India Standards through the hallmarking scheme as of March 2023, which is mandatory in India. There are also estimated to be more than 6 000 diamond processing businesses and 8 000 diamond jewellers in addition to the other types of trade businesses in the sector.

1

108. Analysis of the sector has been included to some extent in IO3 and IO4, and weighting as part of the conclusion is derived on the basis of a prima facie assessment of the extent of implementation of the cash restriction.

### *Preventive measures*

109. The basis for preventive measures for all reporting entities are set out in the PMLA, setting out general requirements for reporting entities to verify the identity of customers and maintain records. More detailed requirements are set out in the PMLA Rules. Reporting entities covered under the PMLA includes banks and other financial services, and DNBFPs consistent with the requirements in the Standards. There are no sectors that have been exempted, except for real estate agents with an annual turnover below INR 2 million (EUR 22 2222) - see R.1 and IO.1.

110. The requirements for some of the sectors were recently introduced into the framework (accountants, company secretariats and other persons conducting TCSP activities). Lawyers in practice carry out activities captured in the FATF Standards only to a very limited extent. General registration requirements have been in place for some time for most sectors that help to identify criminals and it has been recently introduced for VASPs and TCSPs not covered by other requirements. Lawyers, accountants and TCSPs are not subject to AML/CFT work when performing only preparatory acts (see Recommendation 22)

111. Guidelines set out sector specific requirements for FIs, VASPs and most DNFBPs (except lawyers).

### *Legal persons and arrangements*

112. The two types of legal persons in India are companies and limited liability partnerships (LLPs). Companies can be either private or public companies, the latter are almost all listed on the stock exchange, unless they are too small. Section 8 Companies are those set-ups for the purposes of non-profit activities. Legal personality is established when a company is registered at the Company Registry.

113. Other forms of businesses include partnerships (governed by Indian Partnership Act, 1932) and sole proprietorships (governed by State legislation). Indian general partnerships are not considered legal persons for the purposes of the FATF Standards as, while an account held at a financial institution is in the name of the general partnership, the signatory of the account and associated liability rests with the natural person(s) that is(are) the partner(s). Sole proprietorship in India refers to a business carried on by a natural person without establishing an entity with legal personality. Sole proprietorships refer to a business carried on by a natural person without establishing an entity also do not have legal personality according to the FATF definition. Both are common ways of doing business in India due to the simplicity of their establishment compared with the formalities for companies and LLPs. The Central KYC Registry of India, with data from customers of financial institutions, indicates that there are at least 6.8 million sole proprietorships and 850 000 partnerships in India.

114. India does not have separate categories of legal persons called foundations or associations. Non-profit organisations can commonly have the term “foundation” or “association” as part of their name but they normally take the form of companies, societies or trusts.

115. Foreign companies with significant business in India must register with the Company Registry, maintain accounts and update records kept at the Registry.

### Table 1.3. Types of Legal Person in India

| Type of legal person | Total number of registered entities (31 December 2022) | Characteristics |
|---|---|---|
| Private limited companies (PLC) | 2 254 146 | Shareholders of a PLC have limited liability. A minimum of two members and a maximum of 200 members can incorporate a PLC. The transfer of shares is restricted in a PLC, and shares can only be transferred with the consent of other shareholders. Only a natural person can be a director of the company with the statutory requirements of minimum 2 directors and maximum 15 directors. |
| Public Companies | 146 523 | A public company has no restriction on the transfer of its shares, and the number of its members can exceed 200. The shareholders of a public company have limited liability. A public company may be listed or unlisted on a stock exchange. A public company is suitable for large businesses that require significant capital investment and are seeking to raise funds from the general public, however, becoming a public company also involves complying with various regulatory requirements. |
| Limited Liability Partnerships | 294 235 | LLPs a separate legal entity from their partners, which means that the LLP can enter into contracts, sue or be sued in its own name, and own property. LLP partners enjoy limited liability protection, which means that their personal assets are not at risk in case the business faces losses or liabilities. They have more flexible management structures than traditional companies, as partners have more freedom to manage the affairs of the business. LLPs were introduced in India under the Limited Liability Partnership Act, 2008, and have become increasingly popular among small and medium-sized enterprises (SMEs), professionals, and service providers start-ups, and social enterprises. |
| Companies with Charitable aims ('Section 8 Company') | 41 837 | The Government may licence a particular type of company if the primary objectives are conducting charitable, social or other non-profit activities ('Section 8 Company'), according to Section 8 of the Companies Act. Particular features include requirements to reinvestment profits into its charitable work, and a prohibition on the payment of dividends to members. |

Source: Ministry of Company Affairs (registration and filing data)

116. There are four categories of legal arrangements in India which fall within the FATF Standards: Private Trusts, Charitable or Public Trusts (including wakfs), Societies and Hindu Undivided Families (HUFs).

117. 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. There is no strict requirement to establish a trust by a written instrument.

118. The Indian Trusts Act, 1882 defines and governs the law relating to private trusts and their trustees. The Act does not apply to charitable or public trusts (see below). Under India's common law system, a variety of forms of private trusts, including express trusts, are recognised.

- Public charitable trusts are designed to benefit members of the public at large. In addition, states have enacted their own legislation enabling the incorporation and regulation of public trusts.
- 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 Act, 1954. Once dedicated the trust is permanent, irrevocable and inalienable.
- A society may be formed by any seven or more persons associated for any literary, scientific, or charitable purpose, or for any such purpose in accordance with the Societies Registration Act, 1860.

1

- HUFs are legal arrangements, with characteristics consistent with Article 2 of the Hague Convention. They are *express* legal arrangements within the scope of the FATF Standards as they exist as a result of express intentions of the parties, with management of family assets by the *karta* (trustee) for the benefit of the beneficiary/ies.

119. State Authorities may also legislate to allow for the creation of types of Society and Public Trust with specific features in their respective State.

120. There are approximately 107 000 active private trusts in India, and there are approximately 286 000 registered public charitable trusts. In addition, approximately 1 252 000 Hindu Undivided Family businesses (HUFs) filed tax returns in 2023. India does not have available information on the assets held by other trusts. While some private and charitable trusts have tax benefits, private trusts are mostly used for succession planning.

### *Supervisory arrangements*

121. FIs are supervised for AML/CFT compliance by eight public sector regulatory bodies: RBI (banks, OFIs, MVTS), SEBI (securities), IRDAI (insurance), PFRDA (pensions), IFSCA (international financial centre FIs and DNFBPs), NABARD (rural banks – supervised by NABARD but regulated by RBI) and Department of Post or 'DoP' (banking and MVTS in post offices). In addition, stock exchanges play a quasi-supervisory role for securities intermediaries, in addition to the main supervisor SEBI. VASPs are supervised by FIU-IND.

122. DFNBPs are supervised for AML/CFT by the Central Board of Indirect Taxes and Customs – CBIC (DPMS and real estate agents (REAs)); Goa Department of Home and Sikkim Directorate of State Lotteries (Goa and Sikkim Casinos). REAs are also supervised by the Real Estate Regulatory Authority (RERA) for professional accreditation and other regulatory requirements. Self-regulatory bodies are responsible for the supervision of accountants (Institute of Chartered Accountants of India – ICAI and the Institute of Cost Accountants of India) and Company Secretaries involved in providing company formation or other TCSP services (Institute of Company Secretaries of India).

123. The institutional framework for legal persons is set out in the Companies Act. Companies must submit information on the basic and beneficial ownership information in certain circumstances to the Company Registry. A company or partnership's officers are required to provide the documents to the Registrar upon inspection.

124. A specific legal framework sets out the structure of each of the four types of trust or legal arrangement in Indian Law (the Indian Trusts Act, the Wakf Act, the Societies Registration Act, the Hindu Marriage Act, the Hindu Succession Act and State Based frameworks as above). For trusts that have tax consequences in India, trustees are required to hold and submit information on the trust to the income tax department. This includes legal arrangements created according to the legal framework of third countries where they generate income or hold assets in India.

**Table 1.4. Resources of supervisors in India (date)**

| Supervisor | Number of individuals responsible for AML/CFT regulation (where relevant) [FTE] | Number of individuals responsible for AML/CFT supervision [FTE] |
|---|---|---|
| **Financial Institutions** | | |
| RBI | 348 | 1873 |
| SEBI … | 234 | 586 |
| IRDAI | 13 | 60 |
| PFRDA | 14 | 21 |
| IFSCA | 10 | 25 |
| NABARD | 4 | 242 |
| DoP | 30 | 13 453 |
| | | |
| **VASPs** | | |
| FIU-IND | 3 | 3 |
| | | |
| **DNFBPs** | | |
| Casinos | 3 | 5 |
| CBIC (DPMS) | 6 | 134 |
| CBIC (Real Estate) | 6 | 151 |

Source: AML/CFT supervisors

### *International cooperation*

125. International cooperation is routinely sought by India in relation to illicit proceeds generated in India and moved abroad. A number of laws have been enacted and implemented to specifically target the recovery of illicit proceeds laundered overseas, such as the Black Money (Undisclosed Foreign Income and Assets) Act, Prohibition of Benami Property Transaction Act and the Fugitive Economic Offenders Act. India is not perceived to be a destination nor transit country for the laundering of proceeds from abroad, although this is not assessed in great detail in the NRA.

126. India faces a significant TF threat with a major source of funding for most theatres linked to foreign sources. Authorities in India have sought both formal and informal international cooperation in successful TF investigations.

127. Generally positive feedback on international cooperation was received from 17 countries, with some noting the timeliness of responses and quality of requests could be improved.

128. The MHA and MEA are the central authorities for MLA and extradition respectively. Informal cooperation is also coordinated through these authorities as well as on an agency-to-agency basis. Informal cooperation is particularly utilised by the NIA and IB in relation to TF.

1

# Chapter 2. NATIONAL AML/CFT POLICIES AND COORDINATION

## Key Findings and Recommended Actions

### Key findings

a) Authorities in India have a strong understanding of ML/TF risks, and in particular, law enforcement and intelligence authorities involved in CFT have a sophisticated understanding of TF risks, as reflected in the 2022 NRA, various sectoral risk assessments, policies, and cases.

b) A key strength of the Indian system is its continuous domestic coordination and cooperation on AML/CFT issues at both the policy and operational levels at the central and state levels, which has improved since the last assessment. More recently, India has prepared a high-level 2023 Action Plan in response to deficiencies identified in the NRA, and for implementing or monitoring the necessary legal, regulatory and policy changes to mitigate ML/TF/PF risk. The Action Plan includes short-term and long-term goals but does not clearly provide prioritised actions or measurable targets.

c) The NRA draws reasonable conclusions on ML threats and risks relating to modes and channel of laundering. The TF NRA examines India's TF risk exposure by theatres (regional and thematic) which is in line with the TF risk profile for India. However, there are some shortcomings in risk understanding, particularly relating to ML threats arising from trafficking in human beings and migrant smuggling, and ML/TF risks from smuggling and dealing in precious metals and stones, which can be further developed. Understanding on the financial component and ML techniques associated with trafficking in human beings and migrant smuggling should be enhanced, recognising the role of profit making by human traffickers and human trafficking organisations. ML risks associated with smuggling and dealing in precious metals and stones should be further developed given the size of this sector in India.

d) The conclusions of the non-public NRA and sectoral risk assessments are available via FIU-IND's FINGATE portal to all registered reporting entities, and have been communicated to many reporting entities in FIs and DNFBPs across different states in India via an outreach exercise that took place recently. However, there remains a significant volume of reporting entities that have not been engaged.

e) India has put in place measures to exempt real estate agents with a turnover of less than INR 2 million (EUR 22 222), that draw from assessments of risk exposure of real estate agents, and for the provision of simplified due diligence for small income earners, which are important policy measures

given India's context. Real estate agents above the threshold are AML/CFT reporting entities. India has also implemented simplified due diligence measures for "small accounts" to facilitate financial inclusion for low-risk customers and supervisory and national policies evaluate the ML/TF risks associated with these financial inclusion services.

## Recommended Actions

a) Considering the size and diversity of the country, future risk assessment exercises should integrate more nuanced regional ML patterns and trends by threat actors (e.g., organised criminal groups) to support the development of more regionally targeted ML policies and strategies including for investigations and enforcement.

b) India should undertake more comprehensive financial network analysis especially on ML techniques associated with trafficking in human beings and migrant smuggling, to develop its understanding of the ML risks associated with these.

c) India should include deeper qualitative and quantitative data and typologies from domestic and international sources on the ML risks associated with precious metals and stones smuggled into and circulating in India, when undertaking future risk assessments on DPMS and gold and diamond smuggling and the associated ML risks.

d) India should develop its Priority Action Plan so that prioritisation within the broad goals set is clear, and measurable actions are identified for benchmarking the results of AML/CFT measures implemented by specific authorities. This includes developing investigative policies and strategies in addition to devoting more resources for some predicate offences presenting higher ML risk (such as corruption and drug offences).

e) India should continue to monitor market patterns of real estate agents that are exempt from obligations under the PMLA, especially for cases of misuse for ML and TF, to ensure that the exemption for real estate agents with a turnover of less than INR 2 million (EUR 22 222) remain low risk in line ML/TF risk exposure when considering policy objectives for promoting financial inclusion in the housing market.

f) India should broaden access to the NRA and sectoral risk assessments among reporting entities and other relevant entities through enhancing outreach and engagement, and consider releasing a public version of the NRA so that ML/TF risks of India are communicated widely to reporting entities and other relevant entities, including NPOs.

129. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

## Immediate Outcome 1 (Risk, Policy and Coordination)

### *Country's understanding of its ML/TF risks*

130. Overall, authorities in India have a strong understanding of ML/TF risks, and in particular, law enforcement and intelligence authorities involved in CFT have a sophisticated understanding of TF risks, encompassing the assessment of threats and vulnerabilities that are documented in its 2022 National Risk Assessment (NRA) as well as several sectoral and thematic risk assessments on ML/TF risks (see Chapter 1 for the full list). Numerous threat, vulnerability and risk assessments have taken place since the first NRA issued in 2011.[64]

131. The 2022 NRA plays an important role in formulating the understanding of risk across competent authorities at a macro-level, bringing the results of many of the prior sectoral assessments together. The NRA was coordinated by a Joint Working Group (JWG) under the auspices of the Inter-Ministerial Coordination Committee (IMCC) established in 2017 and is represented by a broad range of government agencies (see table 2.1). The NRA (Chapter 1 details the methodology used) takes into account contextual elements of India, such as the size and diversity of the country, sociological origins of certain criminal activity and levels of formalisation of the economy, allowing the NRA to some extent, to incorporate more qualitative data such as regional variation as well as reliance on sources and threats which would better contextualise the transactional data.

**Table 2.1. Inter-Ministerial Coordination Committee**

| Role | Agency |
|---|---|
| Ministries/Government authorities | • Ministry of Corporate Affairs<br>• Ministry of Finance<br>• Ministry of Home Affairs<br>• Central Boards of Indirect Taxes and Customs<br>• Income Tax Department<br>• Ministry of External Affairs<br>• Central Economic Intelligence Bureau<br>• Department of Post<br>• Department of Financial Services<br>• Department of Economic Affairs<br>• National Security Council<br>• National Crime Records Bureau<br>• Niti Aayog |
| Regulators | • Reserve Bank of Inda<br>• Financial Intelligence Unit – India<br>• Securities and Exchange Board of India<br>• Insurance Regulatory and Development Authority of India<br>• International Financial Services Centres Authority<br>• Pension Fund Regulatory and Development Authority<br>• National Bank for Agriculture and Rural Development<br>• National Housing Bank |
| LEAs | • Enforcement Directorate |

[64] In particular the findings in the 2019 Risks, Trends and Methods Report which assessed the ML/TF risks in the financial sector was recently updated in the 2022 NRA exercise and product. The sectoral risk assessments relating to some DNFBPs (such as those related to Legal Persons and Arrangements (2023), Accountants, Lawyers and TCSPs (2022) and the Real Estate Sector (2023)) are more recent which is also reflective of the more developing risk understanding with regards to these sectors. See also chapter 1.

| Role | Agency |
|---|---|
| | • National Investigation Agency<br>• Narcotic Control Bureau<br>• Central Bureau of Investigation<br>• Serious Fraud Investigation Office<br>• Directorate of Revenue Intelligence |

132. The NRA concluded that the most significant ML risks were associated with the predicate offences of fraud and forgery, corruption and bribery and drug-trafficking, and medium risks with smuggling, insider trading and market manipulation illicit arms trafficking and terrorist financing (TF is a predicate offence under the PMLA). Depending on the type of threat, key channels used to launder funds are through cash, offshore instruments, hawala, MVTS, TBML, shell companies and real estate. The threat assessment for the banking sector, the sector associated with the most significant risks, has been rated medium-high on account of the enormity of the number and quantum of transactions in the banking sector relative to any other sector of the economy and the complexity of transactions involved. The major ML threats in the banking sector stem from loan frauds and cyber frauds which exploit weaknesses in risk controls, product features, internal processes, and compliance frameworks. The misuse of bank accounts by shell companies and hawala operators also presents higher risk and the NRA identifies emerging risks associated with new categories of payment and virtual asset service providers (VASPs) in part due to the then existing gaps in mitigation measures.

133. Overall, the NRA draws reasonable conclusions across most ML and all TF threats, drawing on a broad set of qualitative and quantitate sources. However, assessment team considered the possibility that for some crimes, the full extent of the financial component may not have been fully considered for ML. Additional data points that consider not only domestic typologies but also more varied typologies from regional and international sources, would also provide a broader dimension to the understanding of ML risks (see below). The strengths and areas of improvement of competent authorities understanding of risk given they were closely involved in the process, is also reflected below through analysis of the NRA.

### *Money laundering*

134. Considering the size and diversity of the country, reflecting regional variations in ML risks would enhance the usefulness of the NRA. Although regional variation is a data input towards the final risk rating, the NRA could better serve competent authorities as well as reporting entities if regions where certain types of ML threats are more prevalent and the common channels through which proceeds are laundered in these areas are considered. This could also lead to more actionable information in STR filings that law enforcement could use to start ML and TF investigations.

135. One area where the lack of the full extent of the financial component being considered appears to have impacted the overall conclusion, is trafficking in human beings and potentially migrant smuggling, which is assessed in the NRA to be low risk for ML (previously medium risk in 2011). This is based largely on the low proportion of reports filed for related offences against and proceeds of crime from offences relating to[65] bonded/child labour, exploitation of juveniles, and contraventions related the use of passports.[66] While India has recognised the gravity of offences

[65] The NRA took into account the fact that 29 000 cases have been registered under these predicates (which does not include trafficking of persons and exploitation of a trafficked person), and investigations have led to INR 874 million (EUR 9.8 million) since 2018.

[66] Trafficking of persons under sections 370 and exploitation of persons under s370A of the Indian Penal Code is not a predicate crime under the PMLA. See analysis of compliance with Recommendation 3.

relating to trafficking in human beings and migrant smuggling with the expansion of NIA's mandate in 2019 to investigate trafficking in and exploitation of persons that cross state and national borders, the authorities analysis on the financial component relied on the low number of reports and wide patterns of cross border variations were identified, further quantitative analysis of the financial component for this criminal activity was not considered in the NRA. Discussions with federal and state law enforcement investigating human trafficking confirmed that the authorities do not view human trafficking as proceeds generating crime requiring cross border investigations. The fact that the offence of trafficking in persons under the Indian Penal Code is not a predicate offence for ML (R.3) naturally excludes some incidences charged under this offence from being considered in the NRA and may have had an impact on the data and analysis. While the authorities attributed the low number of reports to the low prevalence of crime due to contextual factors such as the low wage nature of labour in India, the NRA also does not sufficiently consider the possibility of other factors such as cases not being registered by police authorities at the state level, as well as the cross border and organised crime aspect of trafficking in persons. This calls into question whether sufficient financial investigations have been carried out, which may also impact the quantum of proceeds being relied on and consequently the overall risk rating.

136. In assessing ML vulnerabilities of sectors, and in the calculation of residual risk, the NRA sometimes places significant weight on the existence of mitigation measures. For example, the NRA assesses vulnerability related to the availability and access to beneficial ownership information as medium in the NRA as a result of the mitigating measures, such as the establishment of the BO registry (2017) and benami transaction prohibition (2016), all of which bring more transparency to purchases and supply chain payments. This is supported by the separate risk assessment on legal persons and legal arrangements conducted in March 2023. However, other factors (see IO.5) indicate that India may need to strengthen its analysis regarding the residual vulnerability of the misuse of legal persons and arrangements so as to provide better clarity on how mitigating measures have impacted residual risks including the use of shell companies in benami ownership of property. Considering the misuse of shell companies remains a high-risk area as confirmed by the NRA, India should continue to focus on developing mitigation strategies in this area.

137. In addition, the medium risk ratings associated with some DNBFP sectors, specifically real estate sector, company secretariates, chartered accountants, and DPMS,[67] are attributed to different mitigation measures and structural reforms in the company formation, real estate, and trade sectors, without more vigorous analysis relating to enforcement and measurement of the effectiveness of the mitigating measures in place. However, particularly with the more recent regulation of these financial gatekeepers for AML/CFT under the PMLA and its implementing regulations and guidelines, mitigation of inherent risks was not or could not be fully measured in the NRA in 2022. An in-depth analysis on compliance by these newly covered DNFBPs should be given more significant consideration in ongoing risk assessment exercises and future NRAs.

138. In other areas, discussions during the onsite with the relevant competent authorities confirms the impact of mitigating measures are factored into the calculation of residual risk, even where this is not described in the NRA. The authorities were able to demonstrate that proceeds of environmental crime appear to have been largely mitigated as a result of action to mitigate predicate risks, for example wildlife trafficking and sandmining.[68] Authorities in India are

[67] The ML risks related to real estate sector, company secretaries and chartered accountants are assessed to be medium, and DPMS to be medium-low.

[68] Establishing State Level Task Forces to implement and review action taken at the ground level. State governments can establish Special Courts to expedite trials related to illegal mining, Geographic Information Systems and similar surveillance technology are used to monitor regional poaching and illegal mining activities.

nevertheless looking to develop the capability of the state enforcement authorities to conduct financial investigation and consequently, deeper threat, vulnerability and risk analysis in this area would support this endeavour.

139. Indian authorities have analysed the ML risks related to both foreign and domestic tax evasion and focus on undisclosed foreign income and assets due to their involvement in ML cases and domestic tax crimes are investigated by the Income Tax Department and domestic tax evasion is not included as a predicate offence under the PMLA. Since the NRA 2011 and various assessments on 'black money,'[69] there have been extensive measures to institute financial transparency that help address tax evasion,[70] and competent authorities demonstrated their understanding of the ways that proceeds are generated and laundered, including through complex cross-border structures.

140. In the context of India, the diamond and precious metal (DPM) is an important sector contributing 7% of India's GDP.[71] Considering the size of the sector and India's leading global role in diamond processing and gold consumption for personal use, the assessment team held significant discussions with various authorities regarding the ML/TF risks presented by this sector. The NRA concludes that risk is medium-low for the sector and medium for smuggling in general after considering several mitigating factors, including the prohibitions on transactions above INR 200 000 (EUR 2 222) in the DPMS sector, dealer registration requirements under the GST, and import and export controls, case studies and typologies (see Chapter 1).

141. While the NRA recognises the threat of gold smuggling across its borders, during the onsite, more in depth analysis, customs seizure data, and case studies and typologies were provided to the assessment team. Discussions with the customs authorities indicated that major organised crime smuggling syndicates has been reduced and an analysis of seizure of gold reveals that gold is being carried by couriers at the behest of retail jewellers who use their small refineries and smelters to melt bullion and manufacture gold jewellery, or individuals smuggling via border crossings (India/Nepal and Bhutan) or airports to take advantage of the customs duty arbitrage. The authorities are aware of the risks avenues for ML through diamonds including valuation risk, TBML, and fraud and have implemented mitigation measures including import duties on polished diamonds and limiting pre-shipment credit for rough purchases through miners and not from rough traders.

142. There have been some case studies indicating sophisticated methods of concealment, suggesting organised crime elements. Data from the Directorate of Revenue Intelligence of India also indicates that seizures of smuggled gold have (except in 2021-2022) been on an upward trend with illustration of routes and modus operandi indicating gold smuggling taking place at India's northeast land borders. Given India's position as a leading consumer of gold and gems and producer of refined diamonds, the authorities should continue to monitor fraud and smuggling evasion techniques with the new regulatory regime for this sector and future iterations of the NRA or other

[69] Defined as undisclosed foreign income and assets. These include the 2012 White Paper on Black Money and eight subsequent SIT on Black Money reports (see Chapter 1)

[70] These include measures to improve the transparency of the tax regime such as the establishment of the Goods and Services Tax (GST) in 2017 and the introduction of the GST Network for digitalising tax collection. To detect tax evasion cases, unaccounted income, and non-files, ITD uses technology to comb the Traces Database. Since Financial Year 2015-16, the ITD has conducted over 60,000 surveys of the data resulting in detection of INR 81.64 billion (EUR 922.5 million) of unaccounted income, made seizure of assets worth INR. 8 billion (EUR , and launched over 11,000 prosecutions resulting in conviction in 300 cases.

[71] Gold is an integral part of religious and social exchanges in India and India has the world's largest cutting and polishing centre for diamonds and is a hub for global jewellery market. See Chapter 1 for more information.

risk assessments for DPMS and gold/diamond smuggling would benefit from the inclusion of broader data and typologies. This would enable investigating authorities to continue to dedicate resources to address ML threats from smuggling of gold and gems in a targeted manner and also help FIs and DNFBPs better understand evasion techniques.

*Terrorist financing*

143. India's TF risk as reflected in the NRA is based on a separate and more detailed TF risk assessment concluded in 2022. The TF risk assessment follows a different methodology from ML, focusing on the source, channels and theatres of terrorism and providing a three-dimensional view of terrorist financing activity in the country. The assessment relies on incidence reports, intelligence, investigations and prosecutions and qualitative analysis by operational experts over several years to understand the movement of money into and within a set of six 'theatres' of terrorist activity. For example, IB had met with NPOs from States taking into account these theatres, to understand their activity and source of their donations. Sources of intelligence are also derived from various cells and working groups representing different stakeholders as well as the MAC/SMAC mechanism (see chapter 1). Separating the six theatres in such a way has enabled India to analyse the sources and channels of movement of funds used to finance terrorists and terrorist activity in more granular way, enabling the development of targeted responses to TF both regionally and thematically.

144. The TF risk assessment identified various modes of terrorist funding, including through sources outside India, organised criminal gangs, extortion, NPOs, fake Indian currency notes, narcotics financing, virtual assets, and illicit arms trafficking, with each demonstrating differing magnitude depending on the theatre. For example, the most frequent and significant source of TF in four of the six theatres of conflicts of India comes from outside the borders of India, while extortion is a major source of funds for terrorist groups in the Northeast and areas affected by left wing terrorism. It also noted instances of abuse of NPOs with links to terrorist organisations and radicalisation, having received funding from foreign countries disguised as funds for charitable activities. Returning foreign terrorist fighters (FTFs) were not considered to be a significant risk area in the context of India due to limited support for ISIL. There are relatively small numbers travelling to conflict zones in view of the size of its population. Competent authorities noted the use of virtual assets to be an emerging trend for TF more generally due to the difficulties faced tracking the funding.

145. India also conducted an NPO risk assessment in March 2023 that built on the TF risk assessment, where the TF threats and vulnerabilities faced to NPOs in the six different theatres were examined and the TF risk determined for each of these theatres. In determining these, the channels of funding as it related to NPOs were considered for each 'theatre.' The findings were fed into the exercise to determine the subset of NPOs at risk for TF abuse. (See IO.10).

146. The TF risk understanding of LEAs and intelligence authorities that investigated terrorism and TF was dynamic and up to date. The authorities were also able to identify the theatres where the TF threat has been declining since the risk assessments were concluded, and as well as observations relating to emerging modes of TF in the theatres where the TF risk remains significant, such as the emerging use of virtual assets.

*ML/TF Risk Understanding*

147. India published its first NRA in 2011 and the 2022 NRA is informed by 12 years of other periodic risk assessment processes and reforms that started in part with the 2011 NRA and the public 2012 White Paper on Black Money. In 2018, India committed to conducting a comprehensive national risk assessment every three years. During this time, India continued to make significant

legislative changes and conducted ongoing typology studies stemming from 2011 NRA and various other threat and risk assessments. This continuing AML/CFT work at a national level reflects the fact that its risk understanding remains uninterrupted over the assessment period. The assessment team also observed that in general, the Indian authorities have maintained a reasonable and dynamic understanding of their ML/TF risks through the continual coordinated sharing of information, risks and trends through the various interagency platforms over the assessment period. Several products such as typology reports and sectoral studies have resulted from these interactions (see Chapter 1). Based on the comparison in the analysis and evidentiary data to support the conclusions, the documented risk assessments, especially the 2022 NRA reflects an overall comprehensive understanding of ML and TF risks.

148. Given the deep and regular participation of India's key policy, regulatory and operational authorities' participation in the preparation of the NRA and the various sectoral assessments since the 2011 NRA, as well as in formulating national AML policies, the findings of the NRA closely resemble the ML risk understanding demonstrated by these authorities. For TF, the LEA, intelligence, and other authorities more directly involved in CFT measures and forums (such as MAC/SMAC) understood the TF theatres and methods with regional variations and supervisors understood the TF RA findings and exposure of their regulated institutions but with less nuance compared to the operational authorities.

149. NRAs and other risk assessments are not public documents (with the exception of the White Paper on Black Money) but following the conclusion of the 2022 NRA there has been outreach (see 2.26 below). The 2022 NRA provides both a threat and vulnerability analysis at a more granular level and the greater accessibility of the NRA and SRAs would allow private entities not just to understand ML/TF risks but also build on them with their own sectoral understanding.

### *National policies to address identified ML/TF risks*

150. The National AML/CFT/CPF Policy Action Plan and Strategy Statement (2023 Action Plan), adopted in 2023, is a high-level national 'whole-of-government' action plan, acting as the document that captures responses to the outcomes of the 2022 NRA exercise. It sets out principles and guidelines for future legislative, executive and institutional reforms to improve the AML/CFT/CPF system. The 2023 Action Plan focuses on prevention, detection, investigation, capacity building, co-operation and outreach.

151. The strength of the 2023 Action Plan is that it is broad and comprehensive in its coverage. India is a large country with regional variations and a wide range of ML and TF that demand national policies to be broad and reflective of the holistic goals that the country seeks to accomplish. However, the country also would benefit from clarity on prioritisation as well as greater specificity in the actions proposed. For example, while the 2023 Action Plan recommends devoting more resources to several different areas of risk and vulnerabilities, it does not identify key focus areas where resources are more critical than in others. Further, the recommendations are very broad and do not provide measurable targets to be able to benchmark the success of measures.

152. India informed the assessment team that each agency has a separate set of achievable targets that it will implement in line with broader AML/CFT policies that will feed into the 2025 NRA exercise. More detailed benchmarks could improve investigative strategies overall as one key benchmark in the action plan is to devote more resources to offences posing high ML risk but little specificity is included on new measures to improve anti-corruption and drug investigations, while more detailed information is provided for combating fraud. Other than agency annual reports that had some specific action items, the assessment team has not had sight of these. Similarly, while capacity building and training on both ML and TF is included in the 2023 Action Plan, the inclusion of more concrete goals that would be useful for policy makers and for future AML/CFT

benchmarking. In terms of CFT, based on the NRA, the 2023 Action Plan focuses generally on devoting more resources without distinguishing between the theatres or methods of TF that are of higher risk. Authorities dealing with terrorism/TF intelligence are aware in which theatres terrorist activity is diminishing and those where terrorist activity remains a concern. Providing more clarity on the allocation of resources according to this understanding may result in the more efficient outcomes.

153. Although the 2023 Action Plan is more recent, India instituted national policies to address ML/TF risks identified prior to the conclusion of the NRA through the interagency IMCC and JWG established in 2017, including in response to the Risks Trends and Methods Report of 2019. Prior to that, the MOF established and implemented AML/CFT policies in response to the White Paper on Black Money (2012) leading to several legislative and administrative reforms. These policies and reforms were implemented over a number of years, including carrying into the assessment period and there have been various other reforms in law, policy and strategy in response to the NRA and other assessments including amendments to legislation such as the PMLA (notification of chartered accountants and company secretaries as DNFBPs) as well as structural changes as shown in the table below.

### Table 2.2. Policies implemented over the assessment period based on identified risks

| Risks identified | Measures |
|---|---|
| Risks from cash-based economy | • Financial inclusion programme – unique bio-metric identification number to each resident (Aadhar), access to zero-balance accounts at no charge (Jandhan).<br>• Development of digital payment ecosystem through cashless digital fund transfer systems.<br>• 2017 ban on cash transactions above INR 200 000 (EUR 2222) for a single transaction, or in multiple transactions related to a single event, or in a single day. |
| Non-visibility of business supply chains | • Introduction of the Goods and Services Tax (GST) in 2017 requiring e-invoices and e-bills and a central data collecting agency allowing transparency of the supply chain through the use of datamining software, to address national and cross-border TBML |
| Risks from cyber-enabled fraud | • Indian Cybercrime Coordination Centre (I4C) scheme in 2020 to develop forensic and technological tools to support LEAs. Seven teams have been established under this that produce produces cybercrime threat intelligence reports, facilitate reporting of cybercrime incidents, facilitate multi-jurisdictional action against cybercrime, engage in forensic analysis through new digital technology and techniques, development of training in cybercrime detection, investigation etc., create platforms for networking and partnerships to respond to cybercrime.<br>• Establishment of the CFCFRMS helpline number for cybercrime victims in 2021, which is taken by the state's cyber-crime cell which connects through a semi-automated system to the financial institution to freeze or trace the transfer of the stolen asset until it is recovered or the trail dies. |
| Risks from bank fraud | • Access to Central Fraud Registry (CFR), a web based searchable database of frauds established in 2016, reported by the banks, to reporting entities to serve as a tool for timely identification, control and mitigation of fraud risk. |
| Corruption risks | • Amendments of the Prevention of Corruption Act in 2018 clarifying liability of senior management in commercial organisations and enhancing punishments for accepting bribes.<br>• Simplification and digitalisation of government tenders and procurement introduced in 2021 and update of manuals for procurement of goods and procurement of works in 2022 to ensure uniformity in the issuance of guidelines. |

| Risks identified | Measures |
|---|---|
| Risks from illicit trafficking in narcotics | • Restructuring of the NCORD coordination platforming 2019 introducing four tiers i.e. at the district, state, executive and apex level. Action Taken Reports (ATRs) demonstrate action taken on the ground which is reviewed at the highest level.<br>• Constitution of an inter-agency Joint Coordination Committee by MHA in 2019 to monitor investigations in cases involving large seizure of drugs.<br>• A special Task Force on Dark net and Crypto currency has been established in 2023 to monitor suspicious transactions related to drugs on Darknet.<br>• Broadening the powers of the border guarding forces and the Indian Coast Guard to be able to interdict narcotics at the borders and at sea.<br>• Policies to mitigate the illicit pharmaceutical products to limit the diversion. |
| Misuse of legal persons | • Task Force on Shell Companies set up in 2017 that compiled a database to identify shell companies found to be used in illegal activities, common directorships in shell companies and suspect shell companies through red flags and monitor action taken by the relevant SRBs.<br>• Between 2017 and 2021, the Registrar of Companies removed 382 875 companies from its register (30% of registered companies) and disqualified 309 619 directors who had not filed their financial statements or annual returns.<br>• Introduction of Companies (Significant Beneficial Owners) Rules in 2018 to make publicly available the details of any natural person indirectly holding more than 10% ownership in a company.<br>• Chartered accountants, company secretaries and other TCSPs notified as DNFBPs and required to file STRs under the PMLA in May 2023. |
| Risks from undisclosed foreign assets | • MLAT Portal, a digital case management system for formal international cooperation, launched in 2022.<br>• Foreign Asset Investigation Units (FAIUs) in 2021 established by CBDT to investigate undisclosed assets held by Indian nationals abroad. |
| Risks from fraudulent loan applications run by overseas fraudsters | • Rules under the Companies Act amended in 2022 to regulate the incorporation of companies, allotment of Director Identification Number (DIN), appointment of directors, transfer/issuance of securities and mergers/amalgamations involving bordering countries. Also, to mandate companies to maintain electronic books of accounts in servers located in India. |
| Risks from virtual digital assets | • VASPs notified as DNFBPs and required to file STRs under the PMLA in February 2023. Detailed guidance issued in March 2023 and FIU-IND Red Flag Indicators developed in April 2023. |
| Risks from emerging technologies | • Establishment by RBI of a FinTech Department in 2022 to foster innovative initiatives such as the Central Bank Digital Currency, to pay focused attention to the Fintech Sector and to facilitate live testing of products or services in a controlled environment through Regulatory Sandbox framework. |
| Improving capacity of ML/TF agencies to reduce overall vulnerabilities | • Development of FIU-IND's FINNET system in 2022 for collection, analytics, and dissemination of financial intelligence using sophisticated risk scoring based on multiple data sources.<br>• Expansion of NIA by 50% more branches and 40% increase in manpower over the last four years. |

154. Policies implemented over the assessment period are in response to identified ML and TF vulnerabilities related to cash, misuse of the banking (especially for fraud), trade, legal and real estate sectors, and undisclosed foreign assets which corresponds largely to the country's main risks. Significant action, particularly after the Supreme Court struck down RBI's circular to require reporting entities to withhold banking services for digital currencies in 2020 as *ultra vires* to the Constitution, such as building forensic technology capability, establishing a semi-automated system to pursue stolen assets of victims of cyber fraud and the inclusion of VASPs as a reporting entity under the PMLA, have been taken for risks relating to cyber-enabled fraud, virtual assets and emerging technology. This is a reflection of the proactiveness of the country in addressing emerging risks. To respond to purchases of real estate with the proceeds of bribery, legislative changes were introduced in 2016 to stop nominee purchases of real estate called "benami properties" where an informal nominee is used to purchase real estate shielding the criminal beneficial owner. Changes were also introduced to stem common money laundering methods related to corruption including the misuse of shell companies via the establishment of a public registry maintained by the MCA (see IO.5) in 2018 and the introduction of cash transaction limits.

155. Significant success has been recorded in relation to some of these actions. For example, India has achieved remarkable improvements in financial inclusion, in parallel to greater reliance on digital payments, in order to address several outcomes relating to financial transparency and

circulation of fake currency circulation, which also contributed to AML efforts. Access to financial services increasing from 35.23% of total population in 2011 with a bank account to 53.14% in 2014 to 80% in 2017 (more current data was not available), helping provide the conditions for a reduction in reliance on cash transactions. Since the establishment of the CFCFRMS helpline for victims to report cybercrime in 2021, more than INR 6 billion (EUR 68 million) has been recovered.

### *Exemptions, enhanced and simplified measures*

156. Given the context of India, exemptions and simplified measures play an important role in helping facilitate access to financial services and other markets for segments of Indian society.

157. India has put in place exemptions from regulated entities' applying the FATF Standards in one area. Real estate agents with an annual turnover of less than INR 2 million (EUR 22 222) are exempted from obligations under the PMLA. The scoping exercise conducted in 2022 is reflected in the 2022 NRA, the 2023 Sectoral Real Estate Risk Assessment, and the AML/CFT/CPF Guidelines for Real Estate Agents issued in May 2023, and is based on the risk exposure of real estate agents that fall below the threshold. The risk threshold was ascertained based on several generalisations of the real estate sector i.e., market rate of 2% brokerage, 24 purchase deals annually of property of at least INR 5 million (EUR 55 555). While there is little discussion of threats within these exercises beyond noting that cash purchases and benami transactions are the ways that money is laundered via the real estate sector and the entities exempted, the understanding of the threats of the authorities during the onsite visit corresponds with the risk exposure of the exempted entities being lower.

158. The purpose of the exemption is so as not to impose an unduly burdensome AML/CFT regime on lower risk micro businesses, to exempt transactions of a lower amount including small agricultural property and to promote affordable housing (see c.1.6).[72] The exemption currently applies to over 90% of real estate agents (see Table 1.2 in Chapter 1).

159. While the 2022 NRA and 2023 Real Estate risk assessment found the inherent risk of ML in the real estate sector to be high overall especially in the primary market (first time sales for new construction or developed properties including commercial) due to the involvement of complex ownership structures involving shell companies or nominee arrangements or offshore investments, overvaluation or underreporting of transactions to evade taxes often made in cash, and weak due diligence related to customer identification, effective mitigation and control measures to bring more transparency into real estate transactions has allowed India to focus on higher risk real estate transactions involving cash purchases and benami transactions while exempting real estate transactions that present lower risk due to the involvement of regulated intermediaries (Registrar of Properties – see following paragraph) and tax revenue reporting.

160. The mitigation measures that reduce the vulnerability of the sector include: income tax reporting requirements such as a tax deducted on sale transactions over INR 500 000 (EUR 55 555) as well as CDD conducted by state land Registrars who are subject to the PMLA. The Inspector-

[72] The 2023 India RE RA evaluated three primary markets for their susceptibility to ML and TF: primary (first time sales for new construction or developed properties including commercial property), secondary (resale of properties), and agricultural. It found that real estate agents are more susceptible to ML in primary sales as they manipulate property prices to accommodate buyers and sellers, and ML in the secondary market involving real estate agents is low as real estate agents are not often used as buyers and sellers are price conscious and usually do not hire real estate agents. Further, regional variations based on urbanization and some regions are considered as higher risk in the primary market (Delhi, Mumbai, etc.) and others medium (Tamil Nadu, West Bengal, etc.).

General of Registration is an intermediary for all the property ownership transfers, which keeps all the necessary documentation (KYC) such as proof of address, proof of identity, photograph of both the parties (buyer and seller). Further, cash transactions above INR 200 000 (EUR 2 222) are banned. Sales tax where the value exceeds INR 3 million (EUR 33 333) are reported to Income Tax Department of India and the sales transactions where the value exceeds INR 5 million (EUR 55 555) are reported to the FIU-IND. The Income Tax department collects Specified Financial Transaction information on real estate transactions. The trend of use of cash in real estate sector has been steadily declining according to the authorities. There are also residency and nationality restrictions on property purchase in India.

161. The exemption threshold for real estate agents should be regularly monitored in line with developing real estate market trends to track if the risk exposure of agents below the threshold become more susceptible to ML.

162. India has also put in place simplified measures for some FATF Recommendations for FIs. To help ensure that low-income earners of the population in India has access to banking, the PMLA allows for simplified CDD in the opening of "small accounts" as defined in the PML Rules as well as other accounts for categories of clients that are low risk. (see c.1.8). The rules do not permit simplified measures where there is a suspicion of ML/TF, where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment.

163. The PML Rules also require enhanced measures based on risk. These requirements are implemented through each regulator in a targeted manner depending on the products and/or sector. This would include enhanced measures for clients of special categories such as non-resident clients, foreign PEPs, clients in high-risk countries, professional intermediaries etc. (see c.1.8).

164. An Expert Committee has been constituted in 2023 to develop a unified KYC policy and has proposed a four-tier customer identification process where documentation sought and verification undertaken will be in accordance with risk. Although this is not yet in place, a more unified risk-based approach may enhance the certainty on risk-based requirements for entities across the country, as long as this does not remove regulators' and regulated entities' ability to institute and implement updated and targeted simplified or enhanced measures, based on changes in the risk situation of different sectors.

### *Objectives and activities of competent authorities*

165. The goals and objectives of LEAs both at the central and state level are generally in line with the ML and TF risks identified in the NRA. While the LEAs from the central government participate directly in the IMCC, there is active information sharing between state and central authorities. The NRA is shared with the LEAs at the state level and information on investigations, risks and trends identified by state-level LEAs are circulated to the IMCC through the MAC/SMAC and other similar mechanisms. Activities addressing ML and TF risks, including prioritisation and allocation of resources, have been broadly consistent with the risk areas identified for LEAs from the central government.

166. Regulators of the financial sector have been conducting risk assessments of their own sector and incorporating risk understanding at the national level reflected particularly the Risks, Trends and Methods Report (2019) and the NRA (2022), using them as a basis for the supervision and monitoring of reporting entities that they are responsible for. Significant observations in these assessments and monitoring are also raised up to the JWG and form the basis of recommendations to update the PML Rules and AML/CFT guidelines for their sector. The two-way sharing of information ensures that these are consistent with the country's risk understanding including risks as reflected in the NRA.

167. Similarly, FIU-IND is cognisant of ML and TF risks and this was evident from the risk-based approach incorporated into the design of the FINNET parameters so that higher risk entities and transactions are prioritised for analysis. Resource allocated to operational analysis is also done on the basis of risks. For example, based on observations of the emerging risks brought on by VASPs, FIU-IND completed seven operational studies on VASPs in India and an SAL study to structure RFIs relating to VASPs in 2023. (See IO.6)

168. Workshops and outreach activities have taken place through which other regulators that are not regularly involved in the IMCC (mostly regulators of DNFBPs) are able to engage on the NRA. These are of particular importance since the NRA is not a public document. DNFBP regulators' risk understanding was broadly consistent with the NRA, although most DNFBP regulators had only recently been brought into the AML/CFT framework and so are yet to define objectives according to risk.

### *National coordination and cooperation*

169. Due to its size and diversity, India recognises the importance of co-operation and coordination amongst its different agencies as well as between authorities from the central government and state-level. This is particularly critical in India as several agencies at central and state-level have overlapping mandates. The ability to co-operate and coordinate both at the policy and operational level ensures that operational agencies are able to function smoothly and in a complementary way.

170. The rotating civil service system in India where civil service officers are regularly rotated amongst agencies as well as across states and between states and the central government contributes to the strong network in the civil service despite the size of the country. The practice of emplacement of officers from agency to another helps to maintain links and share knowledge. For example, Indian Police Service officers earlier posted to NIA subsequently posted with ED, bring with them experience of dealing with TF, since ED also investigates ML where TF is a predicate offence.

171. Different authorities are represented at different coordination platforms, depending on the mandate (see table below). Although some platforms focus on ML and others on TF, many are represented by similar authorities because of the importance given to financial intelligence to both ML and TF, as well as the recognition of the overlaps between ML and TF risks due to there being cases of the funding of terrorist activity from criminal proceeds. The fact that these platforms bring together representatives from authorities with diverse responsibilities i.e., policy authorities, LEAs, regulators on a regular basis to address ML/TF issues in India, supports calibrated mitigation strategies to respond to existing and emerging ML/TF risks. These coordination mechanisms are employed both to address general AML/CFT issues in the country but also more specific risk and threats that arise from time to time (see box 2.1).

## Table 2.3. National coordination platforms

| Committee | Purpose | Representatives | Meetings |
|---|---|---|---|
| Inter-Ministry Coordination Committee and Joint Working Group | Responsible for planning, process and understanding national ML/TF/PF risks, proposing measures for mitigating the risks, examining the progress of the action plan and disseminating the results of risk assessments. | Chaired by Department of Revenue under the MOF. Constitutes policy agencies, (MOF, MHA, MCA, MEA), LEAs (ED, NIA, NCB, CBI), intelligence agencies (FIU-IND, IB, CEIB, DOR-intel), regulators (FIU-IND, RBI, SEBI, IRDAI, PFRDA, DoP, IFSCA), ITD, CBITC, NCRB etc. | 43 meetings over the last five years, although majority took place within the last two years. |
| Multi-Agency Centre | MAC meetings at the national level, and SMAC meetings at state levels, are a key mechanism on national security matters including CT/CFT coordination and sharing intelligence. Intelligence/information at the SMAC may be filtered up to MAC, and up to the JWG/IMCC. | Central TF authorities (NIA, IB, ED), State investigation authorities (e.g. ATS, SIA) | Almost daily meetings over the last five years. |
| CFT Cell | CFT Cell (CTCR Division) has been established in MHA to co-operate and co-ordinate with agencies (e.g., NIA and IB), concerning the development and implementation of CFT policies on operational level and from policymaking perspective. | NIA, IB and relevant authorities. | Regularly |
| Special Investigation Team on Black Money | Task force on policy and operational matters on ML, illicit financial flows, black money, misuse of shell companies etc. It assesses risks and makes policy recommendations through periodic reports, action plans and institutional structures. SIT can also take a coordinating between LEAs in live investigations. | Headed by the Supreme Court. Constitutes FIU-IND, ED, CBDT, MCA, SEBI, RBI, DGGI, and DRI. | 19 meetings over the last five years. Prepared eight reports. |
| Central Economic Intelligence Bureau/ Regional Economic Intelligence Councils | Coordinates information on economic offences such as smuggling, money laundering, tax evasion and fraud, amongst agencies in DOR, intelligence, and enforcement agencies at the national and regional level through an Information Sharing Protocol. (see case study below) | DOR, ED, CBDT, RBI, MCA, CBI etc | 129 meetings over 2022-2023 |
| Narco-Coordination Centre | Three-tier structure at national, state and district level for coordination among drug LEAs and other stakeholders on drug-trafficking related issues, including transnational drug trafficking. SOPs are prepared with other agencies to deal with specific typologies. | Chaired by Dir, NCB and ad hoc participation of ED, ITD, FIU-IND, State Police | 438 meetings over the last five years, although majority took place within the last two years. |
| Fake Indian Currency Note Coordination Group | Started as address the problem of the circulation of fake currency but has shifted focus to other CFT issues after the reduction in threat due to demonetisation. Expanded to coordinate on all CFT matters in the different theatres. | Coordinated by MHA. Constitutes NIA, IB, ED, State CT nodal officers, FIU-IND, RBI. | Eleven meetings over the last five years. |
| Financial Stability and Development Council – sub-committee | Wide scope such as financial stability, financial inclusion etc. Policy issues such as amendments to the PML Rules, use of Aadhar by entities, timely sharing of information by banks with LEAs through a standardized SOP. | Chaired by the RBI Governor and relevant authorities. | Three meetings a year. |
| Central Bank Coordination | Regular meetings of Nodal Officers of Financial Sector Regulator for FIU, between RBI and ED and RBI and FIU-IND to deal with AML/CFT efforts at national and state levels. | Coordinated by RBI or FIU-IND. and nodal officers of financial regulators. | Four meetings a year |
| FIU-India Initiative for Partnership in AML/FCFT | Information coordination through Public-Private Partnership launched in 2022. Facilitate strategic intelligence sharing and knowledge sharing on emerging trends, discussions on best practices in intelligence sharing. | FIU-IND, RBI and 46 REs as well as ad hoc LEAs, sectoral regulators, academic institutions, consultancy firms, think tanks and software developers. | Six meetings since launch. |

### Box 2.1. Coordination through CEIB on TBML

In 2019, the CEIB constituted a group of LEAs to address intelligence relating to the over valuation of the import of rough diamonds and precious metals. The cases shared by CEIB indicated that rough diamonds were being used as a significant mode for ML.

CEIB collated cases of over invoicing of diamonds reported by DRI and Customs and cases shared by REICs. Nine cases were shared in the first meeting held in March 2019 and 23 such TBML cases were shared in seven subsequent meetings between February 2020 and April 2023. Sharing of information amongst agencies and conducting regular review meetings resulted in action against the entities involved.

Follow-up action was taken by the following agencies:

- CBDT - First layer of transactions i.e., parties who made sale/purchases transactions with the entity were identified and found to be bogus entities. Further investigation is under progress.
- ED - Investigation are undergoing for eighteen cases under FEMA and 23 cased for TBML. Two cases have been registered. One investigation involves INR 148.66 billion (EUR 1.7 billion), where INR 105.09 billion (EUR 1.2 billion) was remitted to Hong Kong, China and China. Assets worth INR 459.6 million (EUR 5.1 million) has been attached under the PMLA and investigation is under progress.
- RBI - RBI has twelve banks under scrutiny to verify irregularities in trade finance portfolio involving Buyers' Credit /LoU/LoC etc. RBI has initiated punitive action in respect of deficiencies observed in SWIFT operations of banks.
- MCA - Investigation in nineteen cases has been completed.
- DRI – Prosecution has been filed several cases and others are being examined for possible prosecution.
- CBI – Charges have been filed in one case in December 2022 and investigation is being finalised in another case.
- DGFT – Importer Exporter Code of the entities involved in TBML have been suspended or deactivated in eighteen cases. Remaining cases are under progress.

172. In 2022, the Central Government launched the National intelligence Grid (NATGRID), which is an integrated intelligence database for security and CT purposes. It serves as a valuable intelligence and investigative tool for TF because it contains links to various databases. This database can be accessed by eleven central agencies including the ED and NIA that investigate ML and TF respectively. Since the period between September and November 2023, access to this database has been made available also to State Police. As there are operational symbiotic relationships (e.g., between ED and LEAs on financial investigations, between NIA, IB and State Police on TF investigation and intelligence gathering), the importance of operational coordination is understood by the operational authorities. There is legislation such as the obligation under section 54 of the PMLA for LEAs to "assist" ED with their investigations as well as the processes requiring State Police to inform NIA of any investigation initiated under the UAPA. (See IO.7 and IO.9)

173. The MAC mechanism is also constituted under the WMD Act for coordination on PF and is represented by regulators and LEAs including FIU-IND, RBI, SEBI, IRDAI, PFRDA, CBDT, CBITC, DRI, IB, NIA, DGFT, MEA, MCA and MHA. Intelligence from the MAC is fed to the Inter-Ministerial Working Group (IMWG) which is an inter-agency authority that grants export licence for dual use items in a SCOMET list (See IO.11). The IMWG meets monthly in respect of export licensing cases as well as to discuss PF matters.

### *Private sector's awareness of risks*

174. The NRA 2022 and the sectoral risk assessments are confidential. Although the NRA has been distributed to LEAs and regulators (most of which were involved in the conduct of the assessment), it has not been circulated as a whole beyond government authorities. India also informed the assessment team that SRAs have been shared with relevant government authorities but no further data was provided to detail this. Risk assessment findings, including the conclusions in the NRA, have however been communicated to reporting entities in FIs and DNFBPs via a significant outreach exercise conducted by the DOR, FIU-IND and regulators between December 2022 and May 2023 (Table 2.4). During these sessions a PowerPoint presentation containing a description of the risk-based approach as well as a summary of the conclusions of the NRA was used to communicate the NRA findings. This presentation is also uploaded on FINGATE and thus available to reporting entities registered with the FIU-IND. Presentations also included slides that relate to relevant sectoral risk assessments such as on VASPs.

**Table 2.4. Outreach exercise to REs on the NRA (Dec 2022 – May 2023)**

| Entity | Number of meetings and location | Number of participants | Conducted by |
|---|---|---|---|
| Banking and OFI sector | 3 (Mumbai, Bengaluru, Kolkata) | 317 | RBI |
| Cooperative Banks | 3 | 260 | FIU-IND |
| Scheduled Commercial Banks | 9 | 211 | FIU-IND |
| Real Estate Agents | 10 (Delhi, Karnataka, Maharashtra, Odisha, Gurugram, *virtual* etc) | over 114 | RERA/CBIC/FIU-IND/DOR |
| Real Estate Regulatory Authority | 2 (Kochi and Udaipur) | 90 | CBIC |
| Sock market intermediaries | 12 (Mumbai, Ahmedabad, New Delhi, Kolkata, Chennai, *virtual* etc) | over 363 | SEBI/FIU-IND/DOR |
| Insurance companies | 2 | 144 | IRDAI/FIU-IND |
| Postal sector | 2 | 243 | DOP |
| Payment intermediaries | 3 | 20 | FIU-IND |
| Credit card issuers | 1 | 4 | FIU-IND |
| IFSCA registered REs | 1 (Gandhinagar) | 70 | DOR |
| Casinos | 3 (Delhi, Goa) | over 15 | DOR/ FIU-IND |
| Chartered Accountants, Company Secretaries | 6 (Delhi, *virtual*) | over 17 015 | ICSI/DOR/FIU-IND |
| Bar Councils | 1 (Delhi) | 10 | DOR |
| VASPs | 10 (Delhi, *virtual*) | 183 | FIU-IND/DOR |
| DPMS – All India Gem & Jewelry Domestic Council (GJEPC) | 1 (Delhi and Maharashtra) | 17 | CBIC/FIU-IND |

175. Within this six-month exercise, the authorities were able to reach a large number of entities, not just in Delhi and Mumbai, but also in different parts of India. In addition, the GJEPC (which is not an AML/CFT regulator and whose members deal with import and export of gold and jewellery) also conducted outreach to 4 665 of its 9 500 members across India on the NRA between April 2023

and October 2023. India noted that there has been further engagement by associations of reporting entities to their members but this has not been quantified.

176. India should continue the positive steps it has undertaken communicating the findings of the NRA to various sectors, with a greater focus on higher-risk entities and more recently regulated DNFBP entities. There still remains a large audience that has yet to benefit from these outreach meetings. It has not been demonstrated that those entities where outreach has not yet been conducted, are low risk. For example, three sessions with the banking and Other Financial Institutions (OFI) sector conducted by RBI are a good start but many more sessions are required given the size of the sector. One entity where there has not been any outreach specifically on the NRA is the NPO sector. Based on the assessment team's own observation drawing from discussions with NPOs, while there has been extensive outreach by various authorities on their TF risks and obligations in general, these have not included outreach on the conclusions of the NRA (See IO.10).

177. The assessment team reviewed the detailed PowerPoint presentation of the NRA results that was circulated to reporting entities. Depending on the sector, the richness of the data and analysis related to ML and TF threats and mitigation measures to explain final vulnerability risk ratings would constitute valuable information allowing reporting entities to better build their own risk understanding based on the more comprehensive NRA. Publishing a version of the NRA would also allow reporting entities in the private sector to refresh its own training in accordance with its staffing needs and educate a wider audience. Greater transparency with risk assessments, including findings of the sectoral risk assessments would support India's efforts in ensuring the development of the risk understanding across all REs that is consistent with the NRA.

2

## Overall conclusion on IO.1

The findings in the NRA and the sectoral risk assessments generally demonstrate India's strong understanding of ML/TF risks. Consistent with the risks in the NRA and previous risk assessments, India has implemented a broad range of policy, operational and legislative across measures to address ML/TF risks related to cash, the misuse of the banking, real estate sectors and legal entities. Some gaps in risk understanding, such as that relating to risk associated with human trafficking, can be resolved through more targeted sectoral and thematic risk assessments that consider broader data points and deeper analysis. A more detailed action plan that provides more granular mitigations measures which lay out clear priorities and benchmarks implementation would strengthen responses.

Given India's position as a leading consumer of gold and gems and producer of refined diamonds, India's authorities should continue to monitor fraud and smuggling evasion techniques and associated ML as well as consider collecting further data and typologies so that investigating authorities can continue to dedicate resources to address ML threats in a targeted manner.

There is strong cooperation amongst the authorities in India involved in AML/CFT, with several coordination platforms bringing them together to share financial intelligence and ML/TF trends that support or lead to policy changes.

Outreach has recently taken place with reporting entities on the conclusions of the NRA and sectoral risk assessments given they are confidential. These conclusions have also been uploaded on FIU-IND's FINGATE portal and are available to regulators and reporting entities registered on the portal. However, since there remains a significant volume of reporting entities that have not been engaged.

India is rated as having a substantial level of effectiveness for IO.1.

# Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

## Key Findings and Recommended Actions

## Key Findings

Immediate Outcome 6

a) LEAs routinely access and use financial intelligence and other relevant information in investigations related to ML, predicate offences and TF, demonstrated by case studies and feedback from LEAs.

b) The Indian AML/CFT system features a wide range of sources of financial intelligence and other relevant information, including various types of reporting (STRs, CTRs, etc.), that competent authorities systematically receive from the FIU. This is complemented by LEAs' direct access to databases and records held by reporting entities.

c) FIU analysis and dissemination support the operational needs of competent authorities to a significant extent. The usefulness of FIU products has improved significantly after the introduction of the channels of Priority Intimation STRs and Operational Analysis Reports in 2020 and the operationalisation of the 'Strategic Analysis Lab' in 2021. A system of exchanges of staff between authorities and with the private sector has added to the skills and expertise available. In addition, upgrading the FIU's IT system in March 2023 has equipped FIU-IND with enhanced capabilities to support its analysis.

d) The FIU receives, to some extent, STRs that contain relevant and accurate information. While the quality of STRs has improved over the review period, there remain a number of important sectors and sub-sectors that are not reporting suspicious activity.

e) Lower levels of requests from some LEAs, as well as for tracing and attaching assets, supports the need for FIU-IND to continue to work with LEAs on improving the impact of its work, including by improving the feedback framework between FIU-IND and end-users.

Immediate Outcome 7

a) The ED, the sole competent authority responsible for investigating ML offences in India, is able to investigate and prosecute complex ML activity. The underlying predicate offences are investigated by the respective central and state LEAs. While LEAs are routinely identifying proceeds when investigating predicate offences, it is not clear that they are sufficiently carrying out effective parallel financial investigations and detecting

potential money laundering cases.

b) The ED has a multi-pronged approach in its identification of potential ML cases, identifying potential cases primarily from complaints and open sources, and from predicate investigations. The ED's Technical Circular mandates a broad range of predicate offences to be investigated for ML in accordance with risks.

c) The ED pursues ML related to fraud and forgery in line with predicate crime risks to a large extent, but less so with some other offences such as human trafficking and drug trafficking.

d) India has demonstrated, through case examples, that the ED is able to employ a variety of investigative techniques, and has been successful in investigating cases involving shell companies, TBML, hawala and cash couriers.

e) There have been only 28 ML convictions over the last five years, due to a series of constitutional challenges which were resolved in ED's favour in July 2022 and the saturation of the court system. Although the number of prosecutions and convictions have started to increase over the period of 2022-23, the backlog remains considerable and the current resources are not sufficient to deal with the large number of pending cases.

f) Case studies reflect that the Courts in India have passed dissuasive sentences on natural persons for ML, although the same is not evident for fines imposed on legal persons for ML.

Immediate Outcome 8

a) India has a focus on attachment (seizure) and confiscation of criminal proceeds, as set out in policy and legislation. This is supplemented by a regulatory framework that provides competent authorities with a broad range of powers to identify and seize property and operational mechanisms that support coordination on confiscations between LEAs involved in predicate and ML investigations.

b) India has strong provisional measures for depriving criminals from the benefits of their crimes and helping prevent asset flight through the attachment (seizure) of proceeds of crime, instrumentalities and property of corresponding value at the onset of a ML investigation, with the ED seizing INR 834.1 billion (EUR 9.3 billion) over the last five years. India also seizes large amounts of proceeds and instrumentalities associated with crimes that are not prioritised for ML investigations.

c) Confiscations by ED have amounted to INR 393.7 million (EUR 4.4 million) on the basis of conviction, impacted by the cases still pending before the ML Special Courts, with convictions and confiscation orders not yet finalised. Non-conviction-based measures have been used to confiscate INR 164.97 billion (EUR 1.84 billion) during the period for a small number of cases, including some of significant value.

d) India takes expeditious action to identify and attach (seize) proceeds for criminality and corresponding value which have moved to other countries

through use of MLAs, resulting in attachments of INR 10.8 billion (EUR 119.85 million) abroad.

e) Asset management procedures are implemented at the central level by ED and at the state level by Competent Authorities and Administrators (CAAs) to ensure the retention of value for seized assets of all kinds. Statistics across the CAAs and post-conviction orders of state and district cases are not centrally maintained, impacting the ability of India to readily have a holistic view of confiscations across the country for policymaking and operational purposes.

f) India has a system of capital controls, with the focus on cross-border cash movements directed towards identifying breaches of these controls as opposed to AML/CFT concerns. Nevertheless, a declaration system is in place for incoming cross-border movements and a disclosure system for outgoing movements although no records of disclosures are available for international cooperation purposes.

g) Border agencies work collaboratively to share risk information and collectively have seized INR 5.69 billion (EUR 63 million) of currency falsely declared, or in excess of, the thresholds under the relevant legislation, and applied effective, proportionate and dissuasive sanctions.

## Recommended Actions

Immediate Outcome 6

a) Competent authorities in India should establish a consistent method of tracking the use of financial intelligence in criminal cases (new and ongoing), prosecutions, judicial and other proceedings, as well as for asset recovery.

b) Competent authorities should be required (e.g., through explicit requirements in bilateral MOUs) to provide relevant feedback to FIU-IND on the use of financial intelligence that assists them in performing their duties.

c) FIU-IND should conduct outreach with some LEAs, in particular those dealing with drug offences, to ensure that they are aware and are fully utilising FIU-IND's ability to support more complex financial investigations and asset tracing.

d) FIU-IND should continue to work with relevant regulators and reporting entities to improve reporting by some key sectors and sub sectors, including sectors that have recently been incorporated into India's AML/CFT regime.

3

Immediate Outcome 7

a) India should enhance resourcing for ED and Specialised Courts to be able to swiftly conclude pending ML prosecutions and sustain timely investigation, prosecution and conviction of ML cases.

b) India should enhance the capacity of central and state LEAs to enable them, to more effectively pursue parallel financial investigations into proceeds generating predicate offences, including through more consistent SOPs and other policy measures instituted across States, in view of their important role in identifying ML cases for investigation.

c) India should improve the systemic collection and maintenance of data of ML investigations, prosecutions and convictions for example through expanding the EDOTS system to capture a wider variety of data points.

Immediate Outcome 8

a) India should enhance resourcing for ED and Specialised Courts to swiftly conclude pending ML prosecutions and realise confiscation orders against seized assets, particularly related to convicted ML cases.

b) India should identify operational objectives and key performance indicators to measure the results of confiscation and asset recovery mechanisms implemented by specific authorities under the high-level 2023 Action Plan.

c) India should provide advanced training and capacity development for state and district LEAs, especially CBI and NCB, to further enhance processes and analysis methods used to identify and trace the proceeds of crime in predicate offences.

d) India should improve the systemic collection and maintenance of data on seized and confiscated property, including post-conviction orders, to provide a more holistic view of seizures and confiscations in India to support further policy amendments and risk understanding.

e) India should ensure CAAs and relevant stakeholders are effectively resourced and trained to manage a wide variety of seized and confiscated assets at district and state levels.

f) India should develop and implement procedures for border agencies to systematically record disclosures for intelligence and risk understanding purposes, to flag for further analysis by the FIU-IND and to provide a wider range of international cooperation.

178. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

## Immediate Outcome 6 (Financial Intelligence ML/TF)

179. The key central agencies involved in collecting and using financial intelligence and other relevant information to investigate ML, associated predicate offences and TF in India are the Directorate of Enforcement (ED), the Central Bureau of Investigation (CBI) and National

Investigating Agency (NIA), and the State Police. While the ED is the sole competent authority responsible for investigating ML, both the NIA and State Police investigate TF depending on the scope of the underlying activities. State Police and specific national competent authorities are responsible for conducting investigations into predicate offences specific to their competence. See also Chapter 1.

180. The FIU of India (FIU-IND) plays a key role in India's AML/CFT framework. The FIU's framework allows it to operate in an independent and autonomous manner. It acts as the national centre for the receipt and analysis of STRs and other relevant information such as currency declaration forms (CDFs) and disseminates that information to the above LEAs.[73] In addition to STRs, reporting entities and other private sector entities are required to file the following to FIU-IND:

- Cash transaction reports (CTR) for single or several interlinked cash transactions with value above INR 1 000 000 (c. EUR 11 200) or its equivalent in foreign currency;
- Counterfeit currency reports (CCR) for cash transactions where forged or counterfeit currency notes have been used or where any forgery of a valuable security or document takes place in connection with the facilitation of a transaction;
- Non-profit organisation reports (NPR) for transactions involving receipts by NPOs of value more than INR 1 000 000 (c. EUR 11 200) or its equivalent in foreign currency;
- Cross-border wire transfer reports (CBWTR) for cross-border wire transfers of value above INR 500 000 (c. EUR 5 600) (or its equivalent in foreign currency) where either the origin or destination of funds is India; and
- Immovable property reports which relate to the purchase or sale of immovable property for value above INR 5 000 000 (c. EUR 56 000), and includes information on the total amount of the transaction and details on the parties (identity, address etc.).

181. FIU-IND is the only competent authority that has access to all of the above reporting information and is in a position to disseminate it to other competent authorities. The reports are uploaded, stored and analysed in the FIU IT system called FINNET. FINNET also provides a secure channel for two-way communication between FIU and LEAs through a dedicated module.

182. The analysis for Immediate Outcome 6 is structured such that it focuses on the availability and use of financial intelligence and other information by LEAs; the breadth and quality of STRs; the contribution of the FIU (covering staffing and infrastructure, operational analysis and strategic analysis); and the cooperation, exchange and protection of financial intelligence in the system each under the respective core issue. The findings are predominantly based on statistics on STRs and other reporting received by the FIU and reports sent by the FIU, examples of the use of disseminations, case studies and statistics on ML, TF and predicate cases, interviews with the FIU and LEAs, as well as other relevant information referenced in the analysis.

[73] For incoming physical transportation of currency or BNI foreign currency exceeding USD 5 000 in value or when the aggregate value of all forms of foreign currency exceeds USD 10 000. Sent to FIU-IND on a monthly basis. See R.32.

3

## *Use of financial intelligence and other relevant information*

183. India's AML/CFT system features a wide range of sources of financial intelligence and other relevant information that are available to competent authorities and are accessed and used systematically in investigations related to ML, predicate offences and TF.

184. Information provided by FIU-IND upon request, or spontaneously disseminated, cannot be used as evidence or referred to in any judicial proceedings. LEAs use it as a source of information through which to develop evidence and trace proceeds of crime. In addition, there is a high evidentiary standard maintained by the courts in India, especially with respect to the proof of the foreign predicate offence. This all means that further verification of the grounds of suspicion in FIU-IND information is completed by LEAs before coercive action can be taken, and therefore the information sought by LEAs following a spontaneous dissemination, whether directly by LEAs or via the FIU, is particularly important in context of India's system.

### *Availability of information*

185. Competent authorities including regulators, licencing bodies, and LEAs, have access to a wide range of databases and information sources providing them with access to financial, administrative and law enforcement information as well as financial intelligence (see Table 3.1 below). These are accessible directly and without a court order. Investigating officers can also obtain information relevant to suspected ML or TF directly from reporting entities under provisions of special laws that apply to their respective agency,[74] or through written authorisation from the Courts or the head of a police station under the CrPC.[75] The timeframe for the execution of requests is generally stipulated on the request itself and varies depending on the urgency of the case and the amount of information requested, varying from as little as two hours up to five days. The Central KYC Registry can also be accessed by LEAs through FIU-IND.

[74] For example, the PMLA, UAPA, NDPS, Customs Act, FEMA, FEOA, Black Money Act and Prevention of Corruption Act.

[75] Section 91, for the purposes of any investigation inquiry or other proceeding under the CrPC.

**Table 3.1. LEAs access to sources of information**

| Type of information | Access to LEAs (including State Police, ED, NCB, CBDT and NIA) |
|---|---|
| KYC registry | through FIU-IND by request |
| Records held by financial institutions | by request |
| Registry of property | by request |
| Registry of vehicles | available online |
| Register of Criminal Records (Crime and Criminal Tracking Network & Systems or CCTNS) | available online |
| Central records of economic offences (National Economic Intelligence Network database or NEIN) | Available online |
| Tax data | available online |
| Charge Sheet Records (Interoperable Criminal Justice System or ICJS) | available online |
| Company and Beneficial Ownership Registers (Ministry of Corporate Affairs) | available online |
| Bureau of Immigration | available online |

*Access and use*

186. Overall, a review of case studies provided shows that LEAs have used financial intelligence across a spectrum of investigations relating to ML and TF cases and cases relating to a variety of predicate offences, requesting FIU information, accessing and obtaining information from the other sources. The source of information sought depends on the type of case investigated by the particular LEA.

187. Ordinarily, when the LEAs know the exact account number and the financial institution in which it is held, they can seek the information directly. However, when account numbers and the name of the financial institution is not known and the LEA only has identifiers, such as name, PAN,[76] mobile number, email address, virtual payment address, or passport number, it seeks to identify the accounts or other financial assets associated with such identifiers through FIU-IND, since it has the ability to reach out to a large number of reporting entities in short timespans. In a broader sense, LEAs tend to request information from FIU-IND in cases where the predicate crime or ML modus operandi is more complex, or when cross-border elements are involved. Information requested often includes FIU-IND held information to help establish suspects' financial footprints, identify basic and BO information, and seek cooperation from foreign FIUs at the intelligence gathering stage of an investigation. Case studies demonstrating complex investigations in which information was requested from FIU-IND can be found in boxes 3.1 and 3.2 below.

[76] Permanent Account Number (PAN) – the unique identification number of a taxpayer.

### Box 3.1. Accounts Used for Fraud Based on Illegal Mobile App for Crypto Currency Investment/Mining

Requests for information were received by FIU-IND from state police authorities for information on accounts associated with the names of entities suspected to be involved in fraud. A mobile application was being used to defraud people in the guise of an investment platform for mining of virtual assets. In the course of analysis undertaken by FIU-IND, two entities were identified which were operating on a well-known online store for digital media. Further, these entities were registered with the MCA with a common email address, which was also used as the registered email address by 36 companies with the MCA, out of which, 28 entities had foreign nationals as directors. Based on these investigations, an operational analysis report was prepared and shared with the LEAs with details of persons, addresses, other entities associated with the two entities. The intelligence was used by CBI to register an FIR (first information report) and conduct searches. The information available in the CBI FIR was used by ED in its ongoing investigations. ED has filed a prosecution complaint against 299 individuals and entities (including entities 78 controlled by foreign nationals) in said case before the special court (PMLA), Dimapur, Nagaland. The action undertaken by the ED resulted in freezing of INR 865 million (EUR 9.66 million) held in the bank accounts held by the entities. The operational analysis report was also shared with MCA and RBI for regulatory action.

### Box 3.2. Transactions from Accounts Related to Individual Involved in Terrorism

After a bomb blast in Mangalore in November 2022, FIU-IND received a request from the NIA for information on the financial details and transactions of a suspect. FIU-IND prepared an operational analysis report based on the information gathered from reporting entities and shared it with NIA and Karnataka State Police. FIU-IND analysed the bank statements of the accounts held by the accused and by money mules, used by the accused for moving funds, in order to identify the source of the funds coming into these accounts. The analysis revealed that the accounts held by the accused had received the proceeds of sales of crypto-currency held in wallets with Indian crypto exchanges. Further investigations to follow the money trail revealed that these wallets had received crypto currency from wallets held with an international crypto currency exchange. This indicated that the accused had not bought, but received crypto assets, which were further converted into fiat currency, in the accounts under investigation. Similar modus operandi was followed by another suspect associated with mobile recharge shop, who was paid commission for conducting transactions through the bank account. An amount of INR 0.6 million (EUR 6 701) was obtained through the sale of virtual assets, which was received in the three set of bank accounts, described above, which was withdrawn as cash and handed over to the main suspect. Based on the financial intelligence, the LEAs were able to identify other suspects involved in the blast. The case is ongoing.

188. In simple cases,[77] LEAs usually rely on their own powers to access financial intelligence and other relevant information (see case study in Box 3.3). For example, State Police, either directly or through the EoWs (units who investigate large scale frauds) or Anti-Terrorism Squads or equivalent in each State (who investigate State-wide TF and terrorism, counterfeit currency and organised crime) of each State, are able to seek financial details and other records directly from banks or other financial institutions under level provisions of law (see. R.31).

### Box 3.3 TF investigation into 'Al-Qaeda' cell

A proscribed terrorist cell was involved in identification, recruitment activities and preparation of acts to commit terror attacks, in Lucknow, Uttar Pradesh (UP). The case was registered initially by an Anti-Terrorism Squad, a State counterterrorism unit, and subsequently taken over by NIA in 2021 for investigation. During the investigations, five accused persons were apprehended and explosive materials, other materials required for preparation of IEDs, arms and ammunition were recovered. The investigation revealed that one of the accused, Mr. 'B', was radicalised and recruited another co-accused person 'Mr. F'.

Based on disclosures made by the accused and other witnesses, and documents recovered, it was revealed that on the direction of Mr. 'F', Mr. 'B' donated money to three bank accounts, to support the activities of the terror cell. Bank statements, KYC details of the accountholder, the account opening form (AOF), the account transaction statements, including the details of the counterparties to the transactions, were requested and obtained on the same day by NIA directly from the concerned bank. This revealed that money had been later used for logistical and operational support for active terrorists in Jammu and Kashmir. Mr. 'B' & Mr. 'F' conspired to procure arms and ammunition, which were subsequently recovered from possession of Mr. 'B'. The bank statements and transaction details were used as evidence in the Court.

Six persons were prosecuted in 2022, with TF charges (sections 17, 18B and 40 UAPA) invoked against Mr. B & Mr. F. The accused are presently facing trial.

189. Most LEAs are making a reasonable number of requests to the FIU for information, considering that these requests only represent the cases where LEAs are seeking more complex information as above (see table 3.2 below). The seemingly lower numbers for the ED are explained by its broader powers to obtain information directly under the PMLA, FEMA and FEOA. Furthermore, State Police or the LEA make enquiries to the FIU before cases are submitted to the ED or use their sources of information to make enquiries directly, which are also subsequently available to the ED when they are conducting ML investigations (see IO.7 for broader consideration of the initiation of ML investigations and investigations themselves). The coordinating role played by the IB and its mandate covering 'activities prejudicial to national security' and terrorist/extremist activities explains the larger number of requests coming from the IB. The numbers of requests from some key LEAs, however. appear low in light of the risk profile of the country, in particular the NCB, indicating the need for further awareness raising of the capability of FIU-IND in supporting more complex cases.

190. Although the number of requests by the NIA relating to TF appear to be relatively low in light of the risks and the number of TF investigations conducted over the review period, a given request may contain identifiers which pertain to multiple cases. Requests received from IB also include cases which mention the basis for investigation as terrorist/extremist activities. The relevant findings of investigations by IB are shared with the NIA as the predicate agency. Similarly,

[77] Where the crime was initially registered, the modus operandi was clear and references to bank accounts and other assets were available.

many terrorism-related cases are initially investigated into by the CT wings of the State Police and eventually taken over by the NIA. In such cases, the initial requests for information will come from the CT wings of the State Police and the findings will be shared with the NIA.

191. The rise in number of disseminated linked reports over the review period covered in the table is attributed to the significantly increased capacity of FINNET system to identify linkages between persons and entities in STRs.

### Table 3.2. Number of FIU disseminations in response to LEAs requests

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| IB | 790 | 1 197 | 1 714 | 2 572 | 2 795 |
| State & UT Police | 350 | 407 | 473 | 945 | 997 |
| CBI | 33 | 213 | 144 | 205 | 248 |
| ED | 46 | 168 | 164 | 182 | 154 |
| Military intelligence[78] | 22 | 25 | 67 | 186 | 81 |
| Cabinet secretariat[79] | 15 | 45 | 73 | 85 | 110 |
| DGGI (Goods and Sales Tax Intelligence Service) | - | 20 | 43 | 117 | 195 |
| NIA | 61 | 64 | 98 | 64 | 88 |
| CBIC-Tax Arrears Recovery | - | 2 | 71 | 90 | 48 |
| NCB | 23 | 21 | 25 | 41 | 85 |
| DRI | 18 | 23 | 25 | 21 | 39 |
| CBDT | 4 | 16 | 5 | 5 | 34 |
| SFIO | 2 | 1 | 4 | 37 | 5 |
| MCA | - | 2 | 1 | 11 | 20 |
| CEIB | 12 | 6 | 2 | 2 | 6 |
| **Total** | | | | | |
| Responses to requests, including: | 1 376 | 2 210 | 2 909 | 4 563 | 4 905 |
| STRs | 146 | 1243 | 4025 | 4369 | 5843 |
| Accounts | 7118 | 35823 | 38915 | 78333 | 261312 |
| Other Reports contained | 6 519 | 204 179 | 314 844 | 381 650 | 606 987 |

192. The products disseminated or provided by the FIU (see also Table 3.5) are used to support existing investigations, identify new targets and open new cases, attach assets in some cases, provide feedback to regulators on potential AML/CFT violations, indicate areas for regulatory policy review, and provide guidance to reporting entities on typologies, red flag indicators, and provide feedback on STRs filed. The statistics on receipt and dissemination of reports (see Table 3.7) indicate that the usage of the reports disseminated by the FIU to LEAs varies between 19% and 42% for STRs and can go up to 70% in the case of CTRs. This suggests that the competent authorities are systematically making use of reporting disseminated by FIU-IND both to support ongoing

[78] The disseminations to Military Intelligence are for the purpose of border security and internal vigilance.

[79] The disseminations to Cabinet Secretariat pertain to external security.

investigations and initiate new ones. Some LEAs have also developed their own systems to help assess and store information disseminated by FIU-IND to support its further use (see Box 3.4 below).

### Box 3.4. Use of disseminated information by LEAs

The ED has the sole jurisdiction to investigate ML cases (see IO.7). When FIU-IND proactively disseminates STRs, every STR received is checked against the CCTNS to find whether there is any FIR or predicate offence already registered. Thus, some reports related to 37 ongoing cases by ED. Upon identification of unexplained income/tax evasion by ED, 73 cases have been referred by ED to Tax Authorities to probe the cases in the period under review. Priority intimation STRs are prioritised with all 2693 such reports triggering a preliminary investigation. Since the start of the Operational analysis practice, ED has received 83 Operational Analysis Reports (OARs) from FIU-IND and started an investigation in each case.

Based on an SOP put in place by the Central Board of Direct Taxes (CBDT) for acting upon disseminated STRs, incoming STRs are distributed into three risk categories (high risk to low risk) after data analysis is completed. The high-risk cases are allocated to the Investigation Wing of the Income Tax Department which conducts investigations based on the STRs disseminated. In 3 2215 investigations for re-opening of assessment and scrutiny of income tax returns, FIU-IND STRs were used. All the STRs continue to remain available to the officers of the IW through a search interface and can be used in relevant investigations and enquiries.

The **Central Bureau of Investigation** (CBI) has developed an IT system which processes STRs received from FIU-IND using Artificial Intelligence and Machine Learning algorithms. It classifies STRs based on key parameters such as names, organisations, locations, crime types, and financial transactions resulting in streamlining of information collection, synthesis, and analysis. It also incorporates a crime dictionary, crime-type ranking model, and advanced text analytics to assign a rank to STRs based on the presence of specific crime types. CBI has reported that almost 67% of operational analysis reports resulted in predicate offence or ML investigations.

The **National Investigation Agency** (NIA) has received over 1 000 STRs from FIU-IND over the last five years. Over the review period, 26 STRs were identified which were linked to 15 TF cases registered in NIA. Following this, the STRs were provided to investigating officers to incorporate into their TF investigations, which helped prosecute 134 accused persons, of whom 10 have been convicted and sentenced. Other STRs which were suspected to be related to TF, were analysed by NIA and subsequently incorporated in the database for further reference.

### *STRs received and requested by competent authorities*

193. The FIU receives STRs that are assessed as improving in quality over time and are generally assessed adequate by the FIU as of the onsite visit. Key sectors such as banks and very recently VASPs are submitting material volumes of STRs, however, limited filing by some other important sectors including some FIs and higher risk DNFBPs is having an impact on the STRs that are being received by the FIU and can be requested by competent authorities. Please also see IO.4.

194. The numbers of STRs reporting to FIU-IND has increased steadily across all sectors over the review period from 187 509 in 2018-19 to 421 111 in 2022-23 (with the exception of a fall between 2019-20 to 20-21 predominantly due to the disruption caused by the COVID-19 pandemic). Factors that may have influenced this overall increase include the greater formalisation in the economy,

overall growth in financial transactions and focus on financial inclusion (see Chapter 1), as well as outreach and supervisory activities conducted by supervisors and the FIU.

195. A large proportion of STRs (just under half) are submitted by Public Sector Banks, following by Private Sector Banks (around a quarter). While these sectors do correspond with the sectors that are more vulnerable to ML and TF to some extent (see section 1.4.3 in Chapter 1 and section 5.2.5 in IO4), there is limited reporting from other sectors that have been identified as vulnerable for ML and TF, in particular Non-banking financial companies, money changers , department of posts (MTSS), DNFBPs (especially real estate agents, accountants and TCSPs), and India's IFSC.

196. Imposition of penalty, issuance of warnings, and directions for taking corrective measures have been applied to reporting entities (see IO3). These were generally for failure to register with the FIU, file STRs, or perform CDD appropriately. Most enforcement action was taken against cooperative banks, followed by public sector banks.

197. FIU-IND also conducts ongoing monitoring of compliance of reporting entities as allocated to various divisions ('verticals') organised by type of reporting entity, reviewing the overall compliance of reporting entities with reporting requirements and the quality of received STRs via inspections. These are also used for providing feedback on the quality of STRs filed to the entity-type that they are responsible for. There is also mechanism for incoming STR quality control which rejects reports that are lacking necessary attributes and follows up with the reporting entity to rectify the deficiencies for it to be resubmitted.[80] Issues associated with data quality may also be identified when reports reach the inbox of analysts, who may raise quality concerns with the RE directly.

198. Over the last five years the efforts undertaken by the Indian authorities have helped bringing the numbers of rejected STRs down from 15% to 0.3%.

199. FIU-IND also regularly provides guidance to the reporting entities on data reporting formats, typologies developed based on trends and patterns observed by LEAs, shares strategic analysis, produces as well as sector-by-sector red flag indicators and conducts training through its structure of vertical divisions (see also section on strategic analysis below).

### *Operational needs supported by FIU analysis and dissemination*

200. FIU-IND plays a central role in developing financial intelligence as the only competent authority that has direct access to STRs and mandatory reporting such as CTRs and CBWTRs, filed by over 20 000 entities, and its analysis and dissemination support the operational needs of competent authorities to a significant extent.

201. This section considers FIU staffing and infrastructure; operational analysis; strategic analysis; and FIU support across product type.

#### *FIU staffing and infrastructure*

202. The combined human resources of FIU-IND is 270 employees, including supporting personnel. Seventy-five staff members are posted from a variety of relevant departments and agencies from within the Ministry of Finance, including the CBDT, CBIC, Ministry of Defence,

[80] The FINNET system has in place data quality parameters, failing which reports get rejected automatically. These parameters include checks for ensuring that mandatory fields in the reports are included in the data, as well as corroboration against various government databases, such as PAN, CERSAI etc. An alert goes to the RE with the data quality rejection reason, which prompts the RE to refile the reports after rectification of the deficiencies pointed out.

Department of Telecommunication, State Police Agencies, as well as the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI) and other regulators. The initial tenures may vary between 3 to 5 years, with an option of extension to help retain knowledge and experience.

203. At the centre of the FIU's operational work are 42 managers placed in 10 verticals (teams), headed by 10 senior managers (Additional and Joint Directors). These officials are responsible for directing and overseeing operational analysis, strategic analysis, CFT, support for important cases, coordination with LEAs and regulators, as well as international cooperation. There are specific verticals facilitating receipt of STRs and conducting engagement with allocated reporting entities by sector, such as VASPs, MTSS, NBFCs, cooperative banks, capital market intermediaries, insurance companies, payment system operators etc. In addition, there is a large IT-division of 175 individuals operating the FINNET system. The IT-division facilitates analysis conducted by the system and provides Help Desk support to its users (i.e., from REs, LEAs and the FIU itself). A large proportion of the IT division are trained consultants (analysts) recruited from the banking, securities, insurance and other financial sectors; and from IT- and Fintech companies, bringing important additional expertise and providing analytical support to the verticals.

204. Overall, the variety of different skills and experience brought to the FIU by having analysts and experts from different authorities and private sector entities adds to its capability. This is particularly important given the key role played by IT in the process of producing financial intelligence by the FIU.

205. India uses a bespoke IT system called 'FINNET' to support a number of its internal processes. Starting 2013, FINNET's core processing system, 'FINcore,' began using business intelligence (BI) tools to support the FIU's operational analysis (targeting entities requiring investigation) and strategic analysis (analysis of trends and patterns). In March 2023, India introduced an upgraded version of 'FINNET', that had a major impact on the operation of the FIU. The upgraded system was designed to better facilitate the validation and enrichment of data filed by REs with the help of external data sources. It also had features that allowed for two or more stakeholders to communicate, requesting data and results of analysis and providing feedback. See box 3.5 below.

### Box 3.5. Features of FINNET System (Operational March 2023)

- Employment of Artificial Intelligence and Machine Learning (AI&ML) for advanced analysis of suspicious transactions and case creation.
- Use of Natural Language Processing (NLP) and text mining tools to better analyse textual inputs like Grounds of Suspicion (GoS).
- Use of Application Programme Interfaces (APIs) as connectors to external systems including REs' AML software to facilitate automated reporting of transactions. These APIs shall also be used to capture data from external data sources which may be used for data enrichment during analysis and dissemination of cases to LEAs.
- Use of case management tools for rule/workflow-based case handling.
- Generation of risk scores for individuals, businesses, reports, networks and cases to be able to flag high risk cases/entities/reports for immediate action. The risk assessment is carried out using information pertaining to KYC profile and

transaction patterns obtained from multiple reporting entities, law enforcement agencies and regulators.

206. FIU-IND has access to a wide range of databases and information sources held by various authorities including regulators, licensing bodies, LEAs and access to commercial databases to support its operational and strategic analysis. Access is facilitated through bilateral arrangements including Memoranda of Understanding (MoUs). Access is available on a real-time (online) basis via the APIs of FINNET. The databases are utilised for the purposes of data validation, data enrichment, and for establishing new relationships amongst data points in FINNET.

### Table 3.3 List of External Databases and Resources Accessible to FIU-IND

| Organisation / Database | Data Points |
|---|---|
| CERSAI (Central Registry of Securitization Asset Reconstruction and Security Interest of India) | Centralised KYC information (enabling discovery of all KYC-relationships of an individual or entity). |
| CBDT (Central Board of Direct Taxes) | Information relating to tax filings of an individual or entity including details relating to income range, nature / classification of business, PAN details, and address as per latest income tax return. |
| NPCI (National Payment Corporation of India) | Individual or entity's details on the UPI ecosystem, which may include details relating to account, linked mobile number, virtual payment ID/handle (VPA ID), and related information. |
| CDSL (Central Depositories Services Ltd.) | Individual or entity's portfolio of securities holdings. |
| NSDL (National Securities Depositories Limited) | Individual or entity's portfolio of securities holdings. |
| MCA (Ministry of Corporate Affairs) | Information relating to company incorporation including registration details, identifier details, director / KMP details, shareholding patterns, registered office addresses, and details relating to compliance filings. |
| NATGRID (National Intelligence Grid) | MHA runs host of information from government databases including tax and bank account details, credit/debit card transactions, visa and immigration records and itineraries of rail and air travel. Access to the Crime and Criminal Tracking Network and Systems (CCTNS), a database that links crime information, including FIRs, across 14 000 police stations in India. |
| CEIB (Central Economic Intelligence Bureau) | National Economic Intelligence Network (NEIN) (also referenced as NEOR) database of dossiers and offence cases of economic offenders/suspected tax evaders, based on data received by CEIB LEAs across the country. |
| GSTN (Goods and Service Tax Network) | Database of GST-related details of entities/organisation/persons. |
| RDS (Moody's Risk Database) | Entity KYC details, event details. |
| ORBIS (Moody's Database of Private Companies) | Organization details, BO details. |
| MHA (Ministry of Home Affairs) | Database relating to NPOs which have registered themselves with the MHA for permission to receive donations etc. in foreign currency (which permits access to details relating their annual income and expenditure statements, details of receipts in foreign currency, information about NPOs being put in prior approval category or whose registrations have been cancelled). |
| CBIC (Central Board of Direct Taxes and Customs) | Currency Declaration forms collected by CBIC for incoming physical transportation of currency or BNI (foreign currency exceeding USD 5 000 in value or when the aggregate value of all forms of foreign currency exceeds USD 10 000), sent to FIU-IND on a monthly basis. |
| MEA (Ministry of External Affairs) | Passport database to verify the identity of Indian nationals. |

*Operational Analysis*

207. Depending on the nature of the information received and processed by the FIU by LEAs or intelligence agencies (IAs), the FIU products could take various forms, as described below. Whatever the product disseminated, disseminations rarely contain "raw" STRs. A typical dissemination would represent a package containing several types of reports (STRs, CTRs, CBWTRs,

etc.) that are linked by common identifiers (i.e., names, account numbers, addresses, etc.) as well as enriched by information from other sources via the FINNET.

- **Spontaneous dissemination**, disseminating information on natural or legal persons to LEAs and regulators, for the purposes of new or ongoing investigations and regulatory action.
- **Responses to requests from LEAs,** providing information on identifiers (name, identity number etc.) for natural persons included upon request from LEAs.
- **Operational reports and tactical analysis,** identifying and analysing these and trends (operational analysis reports) or providing multiple reports on a given natural or legal person or group or network (tactical analysis reports).

208. **Spontaneous dissemination** of STRs is undertaken through two sub-processes: selection of STRs for priority analysis and dissemination and determination of recipient LEAs based on the contents of grounds of suspicion and other findings of additional analysis at FIU-IND. Prioritisation is determined on a general priority of order according to a risk score allocated by FINNET, rather than specific categories of prioritisation. Triggers that result in STRs being higher up the priority order are STRs submitted via the channel of priority intimation (i.e., activity identified by reporting entities as potentially warranting a priority response, based on criteria provided by the FIU – see box 3.6); STRs identified for development into operational analyses; STRs which are allocated high risk-scores by the FINNET risk engine; mention of predicate crimes; higher risk jurisdictions or nationalities; suspicious foreign entities; higher risk professions; appearances in watch-lists; turnover[81]; and when there are multiple reports on the same entities or persons.

209. STRs pertaining to terrorist financing, whether reported via the priority intimation channel, or identified through keywords or case tags, are transferred immediately to the CFT vertical who disseminates the STR(s) on the same day (although further analysis may follow). STRs which are filed on accounts of individuals or entities with simple transaction patterns involving a small number of transactions, geographical locations, beneficiaries and originators of transactions, usually require less time to complete the analysis. This analysis usually takes 7-10 days if they are disseminated with tactical analysis reports.

210. Over the period under review, 58% of the priority STRs were disseminated within 7-10 days. The remaining STRs assessed as fit for development into operational analysis, pertained to more complex transactions requiring further analysis usually requiring longer timeframes (up to 30 days).

211. When STRs are filed by REs, and quality checks are completed, STRs are processed by 'FINCORE' to identify linkages including between transactions and common identifiers such as PAN, email, mobile number, GSTIN, and entity names. The FINNET risk engine also allocates risk scores at case, individual and entity level. After this, the STR appears in the inbox of the analyst.

212. The analyst selects STRs based on priority criteria set, such as priority intimation and risk score. The STR is analysed prima facie to determine if the information in it is directly actionable or needs further investigation. In the former case, the analyst may disseminate the STR immediately. In the latter case, the extent of analysis will be determined by the complexity of transactions described in the STR. In simpler cases (for example with a small number of individuals entities and/or accounts and a more limited geographical span), the analysis may involve identification of common sources and destinations of funds, and other identifiers of suspicious activity identified from databases accessible through FINNET, from open sources such as social media platforms, and media references. For more complex modus operandi, the analyst may seek additional information

[81] The total credits and debits observed in the account in question.

from reporting entities such as CDD information, account opening forms, and transaction statements with counterparty details, to identify multiple layers of accounts through which funds are being moved. All the STRs filed by the reporting entities allocated to a vertical are analysed and disseminated by that particular vertical.

213. Over the review period, 432 964 spontaneous disseminations have been shared with LEAs and other competent authorities, most of which contained multiple underlying reports (whether STRs, CTRs, or other reports). These reports have led to the initiation of 38 930 new cases and supported 6 363 existing ones (see table 3.7 below).

214. Association with tax evasion needs lower thresholds of suspicion, such as stand-alone red flags indicating turnovers disproportionate to the profile of the account holder. Therefore, the vast majority of reports go to the tax and customs enforcement authorities, i.e., CBDT, DGGI and DRI. STRs reaching higher thresholds of suspicion which are essential to determine ML and/or the underlying predicate crime, are disseminated to other LEAs. Tax authorities are well equipped in terms of the human and IT-resources to process, analyse and act upon the intelligence shared by the FIU. If in the course of investigation, they determine there is evidence of other predicate offences or ML, the case can be transferred to the ED.

### Table 3.4. Number of reports disseminated spontaneously to LEAs[82]

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| CBDT | 73 025 | 56 147 | 72 018 | 121 075 | 68 755 |
| DGGI | 8 058 | 8 323 | 16 620 | 48 603 | 23 915 |
| State Police | 1 906 | 14 016 | 10 397 | 12 591 | 12 327 |
| ED | 7 493 | 10 588 | 8 171 | 9 207 | 8 022 |
| IB | 3 002 | 6 796 | 9 262 | 7 217 | 3 344 |
| SFIO | 2 957 | 5 333 | 3 645 | 2 570 | 900 |
| DRI | 1 556 | 2 375 | 2 423 | 2 834 | 2 594 |
| CBI | 321 | 849 | 1 049 | 959 | 1 008 |
| MCA | 224 | 520 | 495 | 767 | 267 |
| NIA | 50 | 670 | 184 | 121 | 150 |
| Cabinet Secretariat | 3 | 43 | 12 | 537 | 18 |
| CVC | 13 | 39 | 18 | 39 | 4 |

[82] In this and subsequent tables: the figures might not add up since an individual STR could be disseminated to multiple agencies

### Box 3.6. Priority Intimation STRs

A channel of priority intimation of STRs was established in March 2020 to identify important STRs which require the urgent attention of LEAs. Initially a group of 57 reporting entities, deemed as systemically important, were included in the priority intimation framework. This was expanded in various phases from 2020, to incorporate all banks and systemically important reporting entities from other sectors such as payment aggregators, prepayment instrument provides, car system operations, MTSS and VASPs.

The channel operates via alerts made by the reporting entities to a designated email address within FIU-IND, as soon as an important STR is filed. These STRs are processed on a priority-basis by circumventing the normal procedure of STR dissemination.

Since March 2020, 5 257 STRs have been disseminated via the channel of priority intimation, of which 3 616 STRs were shared by private sector banks, 1 505 STRs were filed by public sector banks, 91 STRs were filed by small finance banks, 38 STRs were filed by Urban Cooperative Banks.

215. The FIU-IND also provides responses to **information requests sent by other competent authorities**. LEAs and IAs routinely request FIU-IND-held information to help establish suspects' financial footprints at the intelligence gathering stage of an investigation from the FIU, as described in the core issue above. LEAs can also make bulk requests and upload their search lists or monitoring rules into FIU-IND databases via FINNET. As noted above, a single dissemination in response to a LEA request often contains multiple STRs as well as other reports, collected on the basis of an identifier (name or identify number for example), as well as KYC and transaction details obtained from reporting identities - pending the nature of the query from the LEA.

216. In August 2020 FIU-IND expanded its operational analysis processes to develop **Operational analysis reports (OARs).** These reports establish trends based on specific modus operandi, predicate crime, geographic trends observed in multiple reports filed;[83] or produce multiple reports on a given natural or legal person (or network) observed in multiple reports filed respectively. OARs identify STRs filed by various REs focusing on specific subjects, analysing them in conjunction which helps establish patterns. OARs include KYC data and transaction details which helps build a comprehensive financial profile of subjects.

217. In June 2022, FIU-IND started a variation of "operational analysis," taking the form of tactical analysis. The process constitutes building a case around a person or entity, establishing conduct and accompanying facts that clarify the reasons behind the commission of a criminal offence.

218. Both operational and tactical reports can be initiated by the FIU-IND itself (e.g., based on strategic analysis), as well as triggered by a request from a LEA, a regulator or other government body. Each dissemination contains packages reports (STRs and other reports) with linkages, for example transactional linkages, common identifies or common directors of legal entities, supplemented with additional information from reporting entities, other databases available and open sources. These reports can be used for a wide variety of purposes: new or ongoing investigations, asset attachments, regulatory action or policy development. A single OAR can be disseminated to multiple LEAs. Over the reporting period 442 OARs have been shared with LEAs and other competent authorities, with growing numbers of them found useful. In several cases,

[83] This kind of analysis is similar to the FATF definition of 'Strategic analysis,' although it can trigger operational or tactical analysis as described further in this section.

these reports have led to further investigation in connection with the concerned predicate offences, ML, and TF. Some relevant case studies are presented below.

### Box 3.7. STRs Pertaining to Post Matric Scholarships

The Government of India provides scholarship schemes to provide financial assistance to economically weaker students. An operational analysis report was prepared based on STRs filed on misuse of such scholarship schemes by a group of closely linked educational institutions, suspected of siphoning funds meant for such students.

Large numbers of accounts were opened through business correspondents of a bank, in the name of persons who did not appear to be genuine students, being too old or too young to qualify for such scholarships. Some accountholders were not domiciled in the states in which the scholarships were offered. Further, common email addresses were found that were associated with the accounts of the beneficiaries and the education institutions. The scholarship amounts were received in the accounts opened in this manner and transferred to the accounts of institutions or withdrawn as cash. Links were observed among institutions through common management, common faculty, common mobile numbers etc. The OAR covered the modus operandi of the scam, KYC and account details of all the subjects and institutes, account opening forms and KYC documents of a sample set of students, bank account statements, and trail of funds as well as other datapoints.

ED initiated an enquiry on the basis of an OAR submitted in November 2022 and search and seizure action was carried out in February 2023 at 22 locations resulting in the seizure of INR 3.6 million (EUR 39 950) in cash, 1200 SIM cards, a Micro ATM machine, 3 000 bank accounts, incriminating documents, and electronic evidence related to the offence and subsequent money laundering. Further, ED shared the information with jurisdictional police authorities and related LEAs basis upon which a FIR was registered against 18 accused persons for committing the scholarship scam and misappropriating government funds.

The ED investigation revealed that the educational institutions in question were engaged in fraudulent practices to secure more scholarships from the government by submitting applications on behalf of ineligible candidates. Through this malpractice, they misappropriated public funds, enriching themselves unlawfully. The investigation estimated the scam to be worth of approximately INR 1 billion (EUR 11.2 million). The perpetrators withdrew cash from multiple states to conceal the origin of funds and to avoid suspicion. Additionally, the institutes maintained undated and pre-signed blank cheque books of student accounts, which were used for transferring and misappropriating scholarship funds according to their own discretion.

As the investigation progressed, three persons directly involved in the scam were arrested and prosecution complaint has been filed against them before the competent court.

*Strategic analysis*

219. Since 2013, FIU-IND has been undertaking strategic analysis using its own databases to identify patterns or trends in behaviour associated with the information reported by reporting entities. In August 2020 the scope was expanded to identify themes or sectors for further operational analyses. Strategic Analysis Group (SAG) of FIU-IND routinely carries out various strategic analyses which further lead to identification of STRs which exhibit similar patterns or trends. This includes identification of new targets for operational analysis from periodic reports such as Monthly RE filing reports and information contained in adverse media reports.

220. In order to make use of the enhanced capability provided by FINNET, FIU-IND established a dedicated Strategic Analysis Lab (SAL) in 2021. SAL is a focused group of data science experts dedicated to data mining and research. The themes of strategic analysis reports are selected based on the objectives outlined in the SAL charter, emerging AML typologies identified by the LEAs, typologies conveyed by REs to the FIU-IND, the latest intelligence gathered through open-source research, and suggestions given by teams within FIU-IND. A total of 76 studies have been undertaken since 2021.

### Table 3.5. FIU Strategic Analysis Products

| Category | Nos of studies |
|---|---|
| Institutional Learning (Trends/Patterns, Vulnerability identification, Open-source intelligence gathering) | 33 |
| Automation Tool (fund-flow analysis tool for large numbers of financial statements) | 11 |
| Research Analysis and publication of typology report | 11 |
| Reporting Compliance | 7 |
| Best Practices | 4 |
| Identification of training needs | 4 |
| Ad hoc (beyond SAL objectives covering assessment of unregulated entities for example) | 3 |
| Risk Rating/Profiling | 2 |
| Red Flag Indicators | 1 |

221. The results of some analyses are shared with LEAs and IAs, as well as with regulatory bodies. Strategic analysis studies have helped inform risk understanding, policy making and refined risk management strategies.

### Box 3.8. Use of FIU Strategic Analysis Products

The strategic analysis report of Counterfeit Currency Reports (CCRs) has been shared with DoR, DRI and IB.

The strategic analysis report of CDF data is regularly shared with ED, CBDT and IB.

The strategic analysis report on MCA data analysis with focus on common registered office address has been shared with MCA, DoR, IB, CBDT and DGGI.

Various reporting guidelines issued as a result of strategic analysis reports are shared regularly with RBI.

The strategic analysis of NPO Transaction Reports led to the finding that mutual funds, government bodies, government schemes etc, are incorporated as trusts or societies and therefore fall under the definition of NPO as per PML Rules, 2005. Based on FIU-IND recommendation, the DoR has changed the definition of NPOs, through amendment to rule 2, in sub-rule (1), of clause (cf) of PML Rules on March 2023.

The strategic analysis report on Virtual Digital Assets and cybercrime types helped FIU-IND has contributed to the decision to subject VASPs to AML/CFT obligations.

The threat analysis for cyber-crimes resulted in issuing guidance/guidelines to reporting entities on cyber-enabled fraud red flag indicators, identification of money mule accounts and typologies.

*FIU support for operational needs across product type*

222. FIU-IND has disseminated a uniform form for feedback to all counterpart LEAs, capturing key points relating to the value of the information provided, the manner in which the information assisted the LEA in its investigation, as well as number of other fields. Feedback is received from LEAs periodically when investigations are concluded. This includes feedback that is received through the feedback tab available on FINNET for the LEAs which enables LEAs to share feedback online. An overview of the feedback is presented in Table 3.7.

**Table 3.6. Number of reports received and disseminated by the FIU [84]**

| | | | 2018- 19 | 2019- 20 | 2020- 21 | 2021-22 | 2022- 23 |
|---|---|---|---|---|---|---|---|
| STR | Received | | 187 509 | 258 603 | 214 942 | 308 501 | 421 111 |
| | Disseminated | Spontaneously | 76 920 | 66 133 | 81 881 | 127 484 | 80 546 |
| | | On request | 146 | 1243 | 4025 | 4369 | 5843 |
| CTR | | Received | 13 975 397 | 15 459 804 | 12 934 750 | 14 275 771 | 14 992 815 |
| | Disseminated | Spontaneously | 2 082 059 | 924 676 | 9 166 886 | 7 301 491 | 4 879 350 |
| | | On request | 5684 | 31 014 | 131 896 | 238 759 | 285 581 |
| NTR | | Received | 439 412 | 940 882 | 791 307 | 816 113 | 838 258 |
| | Disseminated | Spontaneously | 129 760 | 53 718 | 189 | 399 267 | 167 523 |
| | | On request | 98 | 1290 | 8132 | 7930 | 13 321 |
| CBWTR | | Received | 10719253 | 39553003 | 36124141 | 13685250 | 13668380 |
| | Disseminated | Spontaneously | 325 389 | 202 910 | 391 984 | 2 021 419 | 1 048 262 |
| | | On request | 673 | 171703 | 173825 | 132119 | 306387 |

[84] Please note that CDFs, IPRs and CCRs are not included in this table since they are not disseminated as part of STR package.

## Table 3.7. Use of FIU information by LEAs.

| Number of disseminations | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| **Spontaneous** | 76 920 | 66 133 | 81 881 | 127 484 | 80 546 |
| of them found useful (%) | 2352 (**3,05 %**) | 2852 (**4,3 %**) | 13443 (**16,41 %**) | 15600 (**12,23 %**) | 13931 (**17,3 %**) |
| new cases | 466 | 1202 | 12048 | 13365 | 11849 |
| existing investigations | 1689 | 1585 | 1367 | 1002 | 720 |
| assets attachment | - | 1 | 2 | 738 | 894 |
| Other Usage[85] | 197 | 65 | 28 | 1233 | 1362 |
| **Priority intimation reports** | n/a | n/a | 962 | 1613 | 2682 |
| of them found useful (%) | n/a | n/a | 605 (**62%**) | 633 (**39%**) | 865 (**32%**) |
| new cases | | | 589 | 543 | 518 |
| existing investigations | | | 16 | 90 | 347 |
| assets attachment | | | - | 494 | 66 |
| Other usage | | | 109 | 16 | |
| **Operational analysis reports** | n/a | n/a | 101 | 104 | 237 |
| of them found useful (%) | n/a | n/a | 27 (**26,5%**) | 68 (**45,5%**) | 172 (**67,2%**) |
| new cases | | | 25 | 44 | 124 |
| existing investigations | | | 2 | 24 | 48 |
| assets attachment | | | - | 21 | 14 |
| Other usage | | | 10 | 23 | 19 |
| **On Request** | 1 376 | 2 210 | 2 909 | 4 563 | 4 905 |
| of them found useful (%) | 998 (**72,5%**) | 1 513 (**68,5%**) | 2 203 (**75,7%**) | 3 435 (**75,3%**) | 3 824 (**77,9%**) |
| existing investigations | 998 | 1513 | 2203 | 3435 | 3824 |
| assets attachment | | 1 | 1 | 3 | 4 |
| other usage | 2 | 5 | 8 | 14 | 18 |
| **Requests to foreign FIUs on behalf of Indian LEAs** | 289 | 485 | 410 | 483 | 337 |
| of them found useful (%) | 140 (**48,4%**) | 212 (**43,7%**) | 158 (**38,5%**) | 177 (**36,6%**) | 110 (**32,6%**) |
| new cases | 13 | 29 | 25 | 30 | 11 |
| existing investigations | 117 | 179 | 122 | 134 | 94 |
| assets attachment | 1 | - | - | - | - |
| **Spontaneous disclosures from foreign FIUs** | 161 | 181 | 209 | 164 | 182 |
| of them found useful (%) | 114 (**70,8%**) | 119 (**65,7%**) | 140 (**67,0%**) | 110 (**82.1%**) | 125 (**68,7%**) |
| new cases | 62 | 50 | 55 | 57 | 70 |
| existing investigations | 51 | 69 | 85 | 52 | 55 |
| assets attachment | 1 | - | - | 1 | - |

[85] Includes data on information used for identifying assets or criminal proceeds, undisclosed income or for arrests

223. The overall level of positive feedback has been high over the last 5 years, demonstrating the sustained quality of the FIU's work. Although these practices commenced only in 2020, 40% of the priority intimation STRs were found to be useful, and the same figure for OARs, rising from 26.5% to 67.2 % in just 3 years. The figure of spontaneous disseminations found useful averages 10%, which is relatively high and demonstrates improvements in this aspect (usefulness increases from 3% to 17% over the last 5 years). Moreover, spontaneous disseminations in most cases have led to new investigations. It is not clear what drove the significant improvements in feedback on spontaneous disseminations from 2020-21, but this may be due to the implementation of priority intimation reports and/or OARs that supplement the STRs disseminated.

224. In terms of areas where operational support could be strengthened further, statistics on the use of FIU information disseminated or requested are not available in predicate, ML or TF cases where a FIR has been filed or a case that has been prosecuted. More specific feedback from LEAs on where disseminated and requested reports could be improved, and the reasons they were found 'not useful' could identify what further work India could carry out to strengthen the information disseminated or provided upon request by the FIU.

225. In addition, while there is a reasonable proportion of STRs being disseminated that are resulting in asset attachments over the last two years of the review period, some LEAs do not appear to be seeking information from the FIU when tracing assets to the extent expected (see IO.8).

### *Cooperation and exchange of information/financial intelligence*

226. The FIU and other competent authorities systematically co-operate and exchange information and financial intelligence, securely protecting the confidentiality of the information they exchange or use. This is important in India's context, given the size of the country and the number of central and State level authorities that play a role in the AML/CFT framework, and the number of coordinating structures that are therefore also necessary to support the effective operation of the system. Statistics and case studies reviewed by the assessors demonstrate proactive and intensive information and intelligence exchange between FIU-IND and other competent authorities, based on the provisions of PMLA that authorise the Director of FIU-IND to obtain and share information efficiently without requiring a court order or any other form of approval.

227. A senior official responsible for AML/CFT policy in the finance ministry is also temporarily the head of the FIU. This does not impede independence due to the code of conduct all civil servants must adhere to (see R.29). This also helps the prominence of FIU-IND in policy making processes and the mechanisms and processes available for the cooperation and information/exchange of financial intelligence.

228. FIU-IND has entered into bilateral MoUs with LEAs, as well as sectoral regulators (MCA, SFIO, CBI, NCB, CBDT, CBEC, NIA, RBI, SEBI, IRDAI) - which provide a formal framework for enhanced cooperation and protection of information disseminated by FIU-IND from unauthorised use. FIU-IND has institutionalised and held bi-monthly meetings with LEAs and quarterly meetings with sectoral regulators (RBI, SEBI, IRDAI), with a focus on better coordination in information sharing and use.

229. Recruitment of officers from other competent authorities on the basis of deputation is an arrangement that facilitates interagency cooperation and information exchange (see above). These officers have appropriate levels of clearance granting them access to law enforcement and intelligence information, participation in various joint working groups, interagency consultations and review meetings, such as the Special Investigative Team (SIT) on Black Money constituted in 2014, the Joint Working Group (JWG) which cooperates on the NRA exercise, and Inter-Ministerial

Working Group (IMWG) on Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) Licensing. The contracted consultants (analysts) must sign an undertaking making them liable under relevant laws in the event of breach of non-disclosure conditions.

230. FIU-IND is a member and attends regular meetings of several working groups. This includes the MAC, FICN Coordination Group (FCORD), Economic Intelligence Council (EIC) and Regional Economic Intelligence Councils (REICs), convened by the CEIB, and interacts with the agencies of the State governments and Union Territories on regular basis. All the data that comes to the MAC platform is available for FIU-IND and the MAC conducts Strategic Analysis based on its IT-platform. Further, appropriate resources, including representatives of various law enforcement agencies, has been allocated by MAC to address the enhanced cyber/darknet/crypto threats.

231. Suggestions and feedback received from LEAs/IAs have played an important role in finalising the contours of the upgraded FINNET system, building mechanisms for dissemination and exchange of information with other agencies. Enhanced level of confidentiality and security is granted by VPN access only, end-to-end encryption, data leakage prevention, an intrusion prevention system and other in-built functions.

## Overall conclusion on IO.6

Competent LEAs and intelligence agencies systematically access and use financial intelligence and other relevant information in investigations to develop evidence related to ML, predicate offences and TF. The Indian AML/CFT system features a wide range of sources of financial intelligence, including various types of reporting that competent authorities routinely receive and request as they perform their duties.

FIU-IND plays a key role in India's AML/CFT framework, acting as the national centre for the receipt and analysis of STRs and other relevant information, and dissemination of that information. While there are some limitations in the STRs provided by some sectors, including some important sectors, the FIU also receives reports from other sources (such as CTRs) and FIU analysis and dissemination has led to the initiation of a large number of investigations and received increasingly positive feedback from end users, helping demonstrate the sustained quality of the FIU's work. The feedback framework between the FIU and the end users of its information needs to be further strengthened.

India is rated as having a substantial level of effectiveness for IO.6.

### Immediate Outcome 7 (ML investigation and prosecution)

#### *ML identification and investigation*

232. Identifying, investigating and prosecuting ML cases is a national priority for India, which is reflected in the National AML/CFT/CPF Policy Action Plan and Strategy Statement adopted in August 2023. The Enforcement Directorate (ED) is the only competent authority mandated to investigate ML, while Law Enforcement Agencies (LEAs); both Central and State, investigate associated predicate offences. The ED has regional and zonal offices across India, with additional resources focused on regions where more intense criminal activity has been identified.

233. While ED pursues the offence of ML involving the proceeds of crime and instrumentalities in high-priority cases, LEAs launch parallel financial investigations in relation to predicate offences they are responsible for investigating. Predicate offences for which ML investigations and

prosecutions can be pursued is based on the those listed in Parts A, B and C of the Schedule to the PMLA (Scheduled Offences). (See R.3).

*Identification of ML cases*

234. The ED has a multi-pronged approach to the identification of cases that may trigger ML investigations. This is done through seven avenues that are used to identify ML cases (see Table 3.8). i) open sources, ii) referrals from LEAs via ED nodal officers, iii) ED identification through an IT system that monitors predicate cases (the Crime and Criminal Tracking Network & System), iv) the initiation of the ED's director, v) referrals from ongoing cases, vi) FIU disseminations and vii) international cooperation.

**Table 3.8. Avenues for ML identification utilised by ED**

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022- Oct 23 |
|---|---|---|---|---|---|
| Open sources (complaints and tip-offs, media reporting, social networks etc.) | 84 | 249 | 447 | 548 | 605 |
| Direct referrals from ED nodal officers in LEAs | 78 | 227 | 375 | 448 | 396 |
| CCTNS Monitoring | 18 | 65 | 138 | 146 | 182 |
| ED Director's Orders | 7 | 18 | 19 | 28 | 34 |
| Ongoing investigations | 0 | 0 | 0 | 1 | 10 |
| FIU disseminations | 4 | 2 | 0 | 8 | 9 |
| International cooperation | 4 | 1 | 2 | 1 | 9 |

235. The largest number of ML investigations are identified by ED from **open sources**; from the general public, media reporting and information from social networks followed by verification of the information via the CCTNS database and ML reports by LEAs. ED has five regional, 30 zonal and 18 sub-zonal offices in India, and the intelligence units within each of these units monitor open sources of information to identify ML cases for investigation. Complaints and tip-offs can be filed by any member of the public to investigators and officers, who gather intelligence on the ground and ED has the obligation to initiate an investigation into instances of unexplained wealth, alleged predicates that generated proceeds and money laundering. However, these do not form the majority of cases initiated via this avenue.

236. A significant proportion of ML investigations are also based on **direct referrals from ED nodal officers.** Each LEA, both at the central and state level, have one of their own personnel appointed as a nodal officer to the ED. The nodal officer is normally a senior official, with a team of supporting officers who engage in day-to-day operations within the respective LEA, monitor daily operations and input data into the case management system (CCTNS). The role of this nodal officer is to coordinate with the ED on potential predicate offence cases being investigated by their LEA that should be considered by ED for ML investigation. This is done through two prescribed forms (form ML-1 and ML-2), which capture information for the ED on the underlying predicate offences, including the statement of facts, location, persons involved, proceeds involved, proceeds attached, case status, and names of investigating officers, through which potential cases of ML are alerted to the ED by nodal officers.

237. The role of LEAs conducting parallel financial investigations appropriately and comprehensively, and nodal officers at LEAs identifying and communicating potential cases to the ED, are important parts of the chain in India ensuring that ML cases are taken up for investigation based on the ML risks and threats. The process in India for logging new investigations through the First Information Report (FIR),[86] and conclusion of investigations through the Final Form Report

[86] Form IF1 under Section 154 of the Cr.P.C.

(or 'Charge Sheet').[87] provides nodal officers with information associated with the case that they rely on to determine whether cases should be submitted to the ED, as these reports include parameters such as the details of the suspect, details of the property stolen or involved (with the final form including property attached) and its value.

238. In terms of the quality and extent of financial investigations, LEAs demonstrated good knowledge of financial investigation tools and techniques in interviews during the onsite. In addition, LEAs and State Police are attaching (seizing) significant quantities of proceeds (see IO.8), indicating that they are seeking to identify assets as part of their predicate investigations. However, there are indications that LEAs, including the State Police, may not always be conducting their proactive parallel financial investigations to the fullest, for example the more limited outreach by LEAs such as the NCB to the FIU (see IO.6) and based on interviews during the onsite. While LEAs and State Police are guided by SOPs on financial investigations, there was no indication that there was a uniform understanding across authorities on the minimum level of financial investigations that are required beyond attaching (freezing) assets identified upon lodging of the FIR and to what level of sophistication financial investigations should be pursued for different cases. India's efforts to continue building capacity and skills amongst LEAs and State Police conducting parallel financial investigations would have a positive corresponding effect on the subsequent detection of ML.

### Table 3.9 Predicate Offences Registered (FIRs) 2018-23

| Crime types | Nos of Predicate Offences Registered | Offences with proceeds, as indicated based on the FIR lodged |
|---|---|---|
| Fraud and forgery | 1 063 988 | 180 517 |
| Murder | 417 062 | 41 593 |
| Illicit arms trafficking | 321 330 | 92 975 |
| Illicit trafficking in stolen goods | 223 999 | 55 964 |
| Robbery/theft | 209 718 | 92 201 |
| Drug trafficking | 172 855 | 41 892 |
| Extortion | 120 289 | 10 119 |
| Human trafficking/migrant smuggling | 29 018 | 2 550 |
| Counterfeiting/piracy of goods | 15 151 | 2 697 |
| Terrorism/TF | 17 911 | 1 813 |
| Environmental crime | 8 948 | 4 069 |
| Smuggling | 5 238 | 5 238 |
| Counterfeiting currency | 6 815 | 1 162 |
| Kidnapping | 4 049 | 657 |
| Sexual exploitation | 3 575 | 1 494 |
| Insider trading and market manipulation | 12 | 12 |

Source: NRA based on information from FIRs

239. Guidance for the ED on which ML cases should be investigated in India is provided in a technical circular, (see below), which is informed by the NRA. ED provides regular training to nodal and other officers that are involved in the identification of potential cases for ML investigation to help them detect predicate activity that is most likely to result in ML cases being investigated by the ED. Nodal officers draw on these, using their judgement to identify the cases that they believe warrants the initiation of an ML investigation by ED. When this activity is detected by nodal officers, these cases are referred to ED through the 'direct referral mechanism' and multi-agency forums - the MACs and SMACs. Conversely, if the ED conducts a ML investigation that it has proactively

[87] Form IF5 under Section 173 of the Cr.P.C.

investigated, and identifies a predicate offence, it will also share the information and relevant evidence with the appropriate LEA through the nodal officer to investigate the predicate offence. Direct referrals therefore serve as a two-way flow of information between ED and LEAs to identify potential ML cases and uncover underlying predicate offences.

240. Another important source through which the ED identifies ML is through ED regular **monitoring of the Crime and Criminal Tracking Network & System** (CCTNS). The CCTNS is a nationwide online tracking network and case management system managed by the National Crime Records Bureau. It is used by all LEAs to register FIRs filed, investigations and charge sheets for all offences in the country and related information. This information is then available to all other LEAs across India as well as to the ED to be informed of country-wide predicate offences being investigated, attachments and recoveries. The CCTNS is monitored daily by ED and this avenue acts as a secondary monitoring mechanism to identify potential ML cases if any major case is missed through direct referrals from nodal officers within LEAs.

241. Less frequently, ML investigation is also initiated directly through the **ED director's orders,** who is permitted to initiate cases where they relate to law and order, national security, public interest, complex cross-border cases, and where the risk of the dissipation of the proceeds of crime, when they are outside of the prioritisation process (RAMC committee – see below) from any of the seven avenues listed in paragraph above and in table 3.8, or any other source. Some examples involve ML relating to proceeds from stolen national security information as well as Covid-19 fraud during the peak of the pandemic.

242. The ED also identifies ML cases for investigations based on **disseminations from the FIU**. This has occurred directly with ML investigations initiated by the ED on 23 occasions over the evaluation period as a result of disseminations from the FIU. However, as reflected in Table 3.4, FIU-IND has disseminated its operational analyses to LEAs in support of their investigations into predicate offences, which were later taken up for ML investigation by ED, which would not be reflected in table 3.8 above. India was not able to provide data as to the number of FIU-IND disseminations to LEAs that have resulted in ML investigations by ED as it does not keep these statistics.

243. Finally, ML cases are identified from information from MLAs and other types of **international cooperation** as well as based on ongoing non-ML investigations by ED (e.g., under the FEMA), with indications of an ML offence where a specific predicate offence is not yet established.

244. The strength of the multi-avenue approach to identify ML investigations is that, as described above, there is clearly defined responsibility on the ED and to some extent on other LEAs at every level to ensure that ML cases are being identified and investigations are being conducted in India effectively and in accordance with the country's risk.

245. ED's selection of ML cases for investigation is based on its Technical Circular that takes into account ML risks in the country. The Technical Circular was last revised in 2022 to take into account the findings of the NRA. The Technical Circular defines two categories of ML cases for investigation.

246. The first, relates to ML arising out of identified high-risk offences such as offences under the Prevention of Corruption Act involving more than INR 10 million (EUR 112 000), offences under the NDPS Act where the quantity of drugs seized is more than five times the amount prescribed as 'commercial quantity' in the NDPS, cases that have ramifications across multiple states or Union Territories, cases that have serious cross-border implications, cases where there has been a direction by the judiciary or constitutional bodies, bank fraud involving more than INR 250 million (EUR 2.75 million) in proceeds of crime and builder-investor disputes or financial frauds involving more than INR 250 million (EUR 2.75 million).

247. The second category of cases in the Technical Circular is where ML investigations are mandated for predicate offences registered or types of offences irrespective of the threshold. These include some specific predicate offences (Wildlife (Protection) Act, Securities and Exchange Board of India Act, 1992 and Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax, and patterns across offences including offences with 'cross-border implications or economic offences of a 'serious nature.'[88]

248. Cases sent to the ED that are not captured by the mandatory requirement under the Technical Circular, are sent to a Risk Assessment Monitoring Committee (RAMC) which is a committee made up of six senior officers of ED at the central, regional and zonal levels who meet quarterly to takes the decision on whether or not to initiate ML investigation in cases under the non-mandatory criteria submitted to it, based on cases presentations by the respective zones. Cases are then selected for investigation.

249. The selection criteria used by the RAMC is based on a range of factors, such as where influential persons or a large number of victims (i.e., despite the proceeds relating to a corruption investigation falling below the prescribed threshold) are involved. Another example would be drug trafficking cases falling below quantity threshold, however, involving a network of drug traffickers. The RAMC has also initiated cases involving Ponzi schemes, loan application frauds, teacher recruitment scams and illegal mining. Through this approach, India prioritises ML investigations based on the country's risks as well as other considerations such as the complexity and profile of the case so that important ML cases are not missed even if they appear minor (for example if they fall below the monetary thresholds described above). In the financial year 2021-22, the RAMC reviewed 3 265 cases, resulting in 347 ML investigations being initiated.

250. Overall, India has a framework that draws on a number of independent avenues that, taken together, provide an effective system for identifying potential ML cases although it is important that there is confidence that LEAs are pursuing financial investigations to the fullest in order that India's framework allows the ED to optimally identify ML cases for investigation.

*Investigation of ML cases*

251. The functional head of the ED is the Director and investigations are carried out by a team comprising of Deputy Directors (DD), Assistant Directors (AD), Enforcement Officers (EO) and Assistant Enforcement Officers (AEO). As of October 2023, 1 052 investigators were employed by the ED and available for ML investigations. In addition, there are 35 supervisors (Joint Director, Additional Director and Special Director) and over 500 support and administrative staff. Resourcing has increased steadily by about 50% since 2018. Despite this, based on the National Action Plan, ED's resourcing is projected to increase a further three-fold over the next five years. Based on the size and risks of the country and the expected volume and complexity of ML investigations and prosecutions, there is a need to increase the resourcing of ED.

252. ED officers are thoroughly trained, undergoing a mandatory six-week training on entry followed by periodic training on the legal and administrative provisions of PMLA, techniques of investigation, asset tracing capability, drafting of statutory orders (PAO, Prosecution Complaints),

[88] Based on the list provided by India, these are (i) cases where directions have been received from superior courts, the SIT on Black Money, the Central Vigilance Commission as well as other Constitutional Bodies (ii) cases related to TF and naxal activities (iii) cases involving scheduled offences related to waging war against the Indian government, the UAPA, Wildlife (Protection) Act, Securities and Exchange Board of India Act, 1992 and Black Money (Undisclosed Foreign Income and Assets) & Imposition of Tax Act (iv) cases with cross States/Union Territories ramifications (v) cases involving offences with cross-border implications (section 2(ra) PMLA) and (vi) economic offences of a 'serious nature'.

interagency cooperation, skill set of collection of intelligence both by using covert and overt tools, skillset required for trial of the accused and international cooperation.

253. ED's Technical Circulars set out the steps required as part of the investigative process e.g., filing prosecution complaints, arrest and remand, attachment of proceeds of crime, use of formal and other forms of international cooperation, and the use of the FEOA. There is also a Technical Circular that mandates an action plan for all ML investigations, covering modes of investigations, investigative techniques and powers, including special investigative powers. Based on interviews during the on-site visit and case studies presented to the assessment team, the assessors noted that the ED is able to use different investigative techniques, such as controlled delivery, undercover operations and wiretapping and trace funds associated with more complex trails as can be demanded by the complexities of ML investigations (see case study in box 3.9).

254. ED utilises the Enforcement Directorate Offenders Tracking System (EDOTS), a case management system, to log the the Enforcement Case Information Report (ECIR), that includes a wide range of categories, such as: a) scheduled offences involved, b) foreign predicates, c) proceeds of crime identified at the domestic and international level, d) ML typology(ies) involved, e) Search, Survey and Seizure details, f) POC identified and Attached, g) Persons involved, h) MLAs involved, i) confiscation and Restitution Details. Each category is comprised of multiple data points.

255. Throughout the review period, India has investigated over 4 000 ML cases (see table 3.10 below). They include large-scale and complex schemes, involving such techniques as TBML, shell companies, third party ML, and cash couriers, as demonstrated through cases studies.

### Table 3.10. Number of ML Investigations Launched by ED

| | 2018-2019 | 2019-2020 | 2020-2021 | 2021-2022 | 2022-Oct 2023 | Total |
|---|---|---|---|---|---|---|
| No. of ML Investigations | 195 | 562 | 981 | 1 180 | 1 245 | 4 163 |

### Box 3.9. Use of Special Investigative Techniques

Information was received in Zonal Offices on gambling and betting sites that was being circulated on a social media site. ED created an online ID and deposited a token amount through the link provided on the site in order to trace the money trail. Investigators joined conversations on the media site which led to information that victims were being lured to invest money in gambling activities across India. Funds were collected through a Payment Gateway Service and thereafter moved to a company account. Further investigations revealed the company to be a shell company with a nominal share capital and no active business. It was also part of a group of 56 companies with common directors and shareholders controlled by a foreign national. Analysis of the transaction pattern of the accounts of all the companies revealed that although small amounts were credited through a large number of transactions through many bank accounts, the funds were then pooled into a few accounts. The use of controlled delivery and undercover operators led to operations that resulted in search and seizure of documentary evidence. ED also obtained bank documents to complete the investigations.

256. ED investigators have access to various databases and information exchange systems through the secure nodes. These databases include the CCTNS (see above), FINNET (see IO.6) and NATGRID (see IO.1) (see also table 3.1). Since September 2023, access to NATGRID has been

extended to the State Police. Where appropriate, ED also seeks information from oversees open databases. In all case studies India presented, ED investigators accessed the various databases in their ML investigations to gather personal and financial information at various points as part of investigations to develop evidence.

257. Given the importance of close collaboration between ED and other LEAs, LEAs are obliged under section 54 of the PMLA to "assist" ED with their investigations which contributes to coordinated investigations. In addition to the ED nodal officers that are permanently posted in every LEA, for large scale and complex ML investigations, officers from police departments and the Department of Revenue Intelligence (for customs or tax) may be co-opted by ED in investigations for their specific expertise. ED also has officers from all Services and Departments such as Police, Customs, Income-Tax, GST etc which enables ED to benefit from their respective domain knowledge, expertise and back-end coordination with their respective parent departments.

258. ED's participation in multi-agency forums like MAC and SMAC facilitates the establishment of joint investigations and operations with various agencies such as CBI, NIA, CBDT and State Police. Case studies reflect that these have resulted tangible results (see Box below). Overall, the ED is capable of investigating complex and large-scale ML cases (see also case on informal banking and hawaladars below).

### Box 3.10. Joint Investigations: ED and other authorities in cross-border case

A case was registered by Delhi Police against a hawala operator based in Dubai for remitting proceeds of offences of cheating, forgery and extortion, using illegal channels since 2020 estimated at INR 2.15 billion (EUR 23.65 million). The hawala operator was investigated and his movements were jointly monitored by Delhi Police, by the ED and ITD. The authorities accessed his communication systems that revealed that he planned to visit Delhi in 2023. When he arrived at the hotel to meet some associates, a joint raid was conducted by the three authorities. The suspects were apprehended with incriminating documents and messages in their mobile devices recovered.

Cooperation amongst the authorities involved informal meetings and discussions about proposed plan of action so as to coordinate searches and arrests. The authorities accessed several databases as part of their investigation, including the CCTNS, MCA, NATGRID, bank databases and open sources of information. The authorities used intelligence and surveillance to monitor the movement of the suspects. Investigations revealed that cross border hawala movement of INR 312 million (EUR 3.3 million) were executed through a web of transactions effected by 24 companies opened by benamidars (illegal nominees), and cross-border remittances were made in the guise of payment for import of services.

Interrogation of the suspect was also conducted jointly, leading to information regarding the suspect's criminal network, modus operandi of the illegal hawala activities and identification of proceeds of crime. The hawala operator was arrested and ED obtained attachment orders on the proceeds of crime. The total proceeds of crime laundered by the hawala operator was INR 312 million (EUR 3.25 million). In total for all associates, the proceeds were INR 2.15 billion (EUR 22.5 million).

India obtained information from the UAE through FIU-IND via EGMONT channels.

### Box 3.11. Case Study – ML investigation involving Hawala

In 2018, ED was investigating a case under the FEMA which led to information that the mastermind of a criminal network and his associates had established a web of shell companies in India and abroad (450 entities in India; 104 entities mostly in Dubai and Hong Kong, China; and 102 entities based on forged documents). The Economic Offences Wing of Delhi Police registered predicate offences relating to fraud, forgery, counterfeiting of documents and organised criminal conspiracy, based on a preliminary inquiry from ED.

It was uncovered that the scheme involved recruiting dummy directors for shell companies. Fictitious persons were created using fabricated photographs and ID documents for the purpose of company incorporation, opening bank accounts and for fraudulent transactions.

Key accomplices managed offices, recruited employees and handles bank account transactions as per the mastermind's instructions. The network used circular trading and provided accommodation entries to facilitate domestic operations. Fictitious turnovers from multiple accounts of shell companies were created.

The mastermind also created dummy travel companies to route money overseas to countries including Dubai, Hong Kong China and Singapore. These overseas entities sent forged documents related to fictious foreign travellers to authorised forex dealers to facilitate foreign exchange remittance.

Investigations included accessing the MCA portal, income tax returns, passport and travel details from the Bureau of Immigration, STR and CTR information from FIU as well as bank account information from banks.

The investigation uncovered INR 5.65 billion (EUR 63.11 million) generated from ML activity. An attachment order for INR 800 million (EUR 9 million) was confirmed by the Adjudicating Authority and charges have been filed against the mastermind. Prosecution complaint was filed in 2020 and 2022. The hearing regarding the charges to be framed against sixteen suspects, including the hawala operator, as well as bail hearings took place in 2023 and are on-going.

This case also led to a series of investigations into at least two other Hawala operators and their associates who were using similar methods.

## *Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies*

### *Types of ML investigated*

259. In general, the majority of proceeds of crime are generated through predicate offences committed in India, and laundered funds are either integrated in the country itself or are siphoned off to offshore locations. Based on the NRA, the country's ML threats relate to predicate offences such as fraud, corruption, illicit drugs and arms trafficking, and ML methods involve mostly banks, shell companies, TBML, hawala, and cash couriers.

260. All ML cases investigated over the review period, involved over 22 000 individual predicate offences (FIRs), the vast majority of which are serious offences consistent with the predicate risks identified (please see Table 3.9). Fraud, forgery, corruption, participation in criminal groups, and

illicit trafficking in drugs are the predominant predicate offences that were investigated for ML by ED throughout the review period.

261. The low number of ML cases related to drug trafficking (over the evaluation, 220 cases were investigated with 27 prosecutions and five convictions) may be attributed to the threshold related to the quantity of drugs seized to mandate an ML investigation. India has noted that this is mitigated by the fact that the NDPS allows the tracing and freezing of illegally acquired property associated with illicit narcotics. Although human trafficking is not a designated category of offence, criminal conduct relating to trafficking in human beings and migrant smuggling, and sexual exploitation fall within that range and have contributed to 54 cases. The relatively low number of related ML cases is attributed to improvements needed in understanding the financial components and ML techniques associated with these crimes (IO.1) and the overall underreporting of this crime.

### Table 3.11. ML Investigations By Underlying Predicate Offence Category (2018-Oct 2023)

| Predicate Crime Type | No. of ML Cases registered by ED (ECIRs) * |
|---|---|
| Fraud and forgery | 3 396 |
| Corruption and bribery | 1 314 |
| Participation in an organised criminal group and racketeering[3] | 1 208 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 220 |
| Illicit arms trafficking | 93 |
| Environmental crimes including Biological Diversity Act, Wildlife Protection Act, Protection of Plant Varieties and Farmer's Rights Act etc. | 95 |
| Terrorism, including terrorist financing | 83 |
| Extortion | 79 |
| Trafficking in Human Beings & Migrant Smuggling | 43 |
| Sexual Exploitation including sexual exploitation of children | 11 |
| Kidnapping, illegal restraint and hostage taking | 3 |
| Murder, grievous bodily injury | 48 |
| Illicit trafficking in stolen and other goods | 44 |
| Smuggling | 46 |
| Counterfeiting and piracy of products | 26 |
| Robbery or theft | 19 |
| Tax Crime (Only pertaining to Black Money Act cases) | 20 |
| Insider Trading | 23 |
| Counterfeiting currency | 9 |

* An Enforcement Case Information Report (ECIR) is similar report to the FIR used by the ED when an ML investigation is initiated. Note each ML investigation (and therefore each ECIR) may comprise multiple categories of predicate offences.

### Box 3.12. Investigations into key typologies

**Investigation into Shell Companies**

Two FIRs were registered by the CBI against a company for offences under the Indian Penal Code and Prevention of Corruption Act for criminal conspiracy to defraud Indian public sector banks and to launder proceeds amounting to INR 146 900 million. Initially, ED logged an ECIR and conducted its intelligence during 2017, which eventually led to a search operation conducted in 2018 of a secret godown (warehouse or storage area) where documents and digital records of shell companies and their directors were uncovered and uncovered the complex scheme and initiated the ML investigation. The directors were employees paid small amounts to lend their names to these companies.

Two hundred and forty-nine shell companies were created in India and another 96 shell companies were created abroad, for a total of 345 companies, with nominees and fabricated financial statements. These were created to induce banks to sanction higher credit limits, and loan funds were then obtained through bank fraud and diverted through complex transactions to be invested in assets in the name of the shell companies located abroad in the UK, USA, Nigeria, Panama and other jurisdictions. The suspects beneficially owned these shell companies in India and abroad.

Proceeds were identified in multiple jurisdictions (UK, USA, Nigeria, Panama, BVI, Barbados etc) which amounted to INR 145 billion (EUR 1.61 billion) and fifteen provisional measures (attachment orders) were issued. Assets valued at INR 47 billion (EUR 520.3 million) were secured in India and another INR 97.8 billion (EUR 1.07 billion) in several jurisdictions, such as Nigeria and UK, for moveable and immoveable properties, including shares, oil rigs, vessels and aircraft.

Considering the complexity of the investigation and cross-border movement of funds, 21 outgoing MLA requests were issued to many jurisdictions, including the aforementioned, with 15 have been sent for execution of attachment orders and 5 were for providing legal assistance by collecting financial and other forms of evidence to be used for the ML investigation and prosecution in India. Thus far, India received 9 responses.

Five prosecution complaints have been filed during 2018 involving 194 natural and legal persons and 4 individuals have been declared as fugitive economic offenders.

**TBML Investigation**

CBI registered an FIR of an allegation by a public sector bank alleging that some bank employees in collaboration with others, had fraudulently issued Letters of Understanding (LOUs) amounting to INR 64 982 million (EUR 725.83 million) without following the required procedures. The LOUs were used to raise buyers' credit and fund accounts of the bank through overseas branches of Indian banks. The funds obtained through these fraudulent transactions, which were siphoned off through complex transactions and laundered.

The ED initiated ML investigation under PMLA in 2018 and it was discovered that the unauthorised LOUs were not used for genuine transactions but were instead siphoned off by Mr. A, his affiliates, and other co-conspirators by laundering the proceeds of crime through various entities and overseas companies controlled by Mr. A. These overseas companies were found to be dummy companies created to facilitate the projection of tainted funds as untainted, which was found to be the main method of laundering of proceeds. To avoid

suspicion, import and export of gold and jewellery were shown against remittances and transfer of funds. However, the gold and jewellery were re-circulated to assist with the re-integration of proceeds of crime. The fictitious import-export transactions were then used to show inflated turn-over of the companies to access a higher credit limit from banks.

Mr A did not show up when summoned by the ED and the ED filed an application under the Fugitive Economic Offenders Ordinance to declare Mr. A a fugitive economic offender and confiscate his properties. 18 Letters Rogatory (LR) under PMLA were sent to different countries (USA, UK, Singapore, UAE, South Africa, Hong Kong China, France, Armenia, Belgium, China, Japan, Malaysia, Bahrain, Russia etc.), requesting assistance for investigation and information. Based on the Extradition Request by ED and CBI, Mr. A was arrested by the UK. A extradition trial is in its final stages in the UK courts.

Based on the investigation, properties worth approximately INR 18.73 billion (EUR 206 million) were provisionally attached through 12 different PAOs under the PMLA, and multiple seizures amounting to INR 4,897 million (EUR 54.7 million) were made. the Special Court ordered confiscation of free hold properties of approx. INR 3.297 billion (EUR 37 million) belonging to Mr. A.

ML charges were preferred against Mr A and 26 others, including the employee of the bank. Mr. A's family members and other associates were also found to be actively involved in money laundering and concealing the proceeds of the crime as many of them controlled corporate vehicles for facilitating concealment and projection of proceeds of crime.

**Investigation into Cash Couriers**

ED initiated an investigation in 2022 on the basis of a case registered by the State Police for criminal conspiracy and cheating where an online platform was engaged in illegal gambling through different live games (e.g., cricket, football etc). The online platform operating all over India was engaged in betting activity, which according to processes and analysis methods used to calculate the proceeds generated from criminality were estimated at INR 4.5 billion (EUR 47.5 million) monthly. Investigations revealed that the operators and employees of the online platform were based outside India. Further, cash couriers were engaged for collecting hawala money and for payment of cash of INR 5.7 billion (EUR 60 million) to local senior public officials and politicians as bribes, for ensuring 'smooth operations' of the betting platform.

Mr Y was found to be handling the financial operations of the online platform and ED received information that he would be delivering cash to politicians through Mr Z. ED intercepted this delivery and recovered the cash consignment of INR 53.9 million (EUR 600 000).

*Prosecution of ML cases*

262. Once a prosecution complaint is filed by ED, the prosecution of both the ML offence as well as the predicate offence is heard by a Special Court established by section 43 of the PMLA. ED has around 173 dedicated prosecutors who specialise in ML and receive appropriate training. The numbers of prosecutors have been increasing steadily from 110 in 2018. Where necessary, solicitors are also retained to represent the State.

263. As at the end of the on-site, there were 104 Special Courts in India in total. The numbers of Special Courts have been increasing steadily from 66 in 2018. Their regional distribution is dependent on the various levels of economic and criminal activity in different areas, for example, there are one or two Special Courts in smaller states and up to 25 Courts in Delhi. Each Special Court currently oversees on average twelve cases per annum. During the course of a trial, courts can instruct MLAs to be issued or investigative measures to be carried out as required. Authorities

indicated that simple cases take between fifteen to eighteen months until conviction, while complex cases may take up to five years.



### Table 3.12. ML Prosecution

| | 2018-19[89] | 2019-20 | 2020-21 | 2021-22 | 2022- Oct 23 | Total |
|---|---|---|---|---|---|---|
| ML investigations launched | 195 | 562 | 981 | 1 180 | 1 245 | 4163 |
| ML investigations where a decision was taken not to investigate | 39 | 17 | 12 | 18 | 46 | 132 |
| Prosecution Complaints filed | 216 | 51 | 130 | 144 | 323 | 864 |
| ML Cases Convicted | 4 | 4 | 1 | 3 | 16 | 28 |
| ML Cases Acquitted | 1 | 0 | 0 | 0 | 0 | 1 |

Source: *EDOTS*

264. While the number of ML investigations have been increasing over the period under review, the number of prosecution complaints have not caught up accordingly (while noting the timing of investigations and prosecutions may differ significantly due to the delay between the start of an investigation and filing the Prosecution Complaint (PC) which could take several years). On average, 20% of all ML investigations were prosecuted, with 3% reaching the conclusion to not prosecute. ED has faced only one acquittal during the review period, although the number of ML cases convicted is relatively low with only 28 cases convicted for ML over the evaluation period. Although the conviction rate stands at almost 97%, there are a number of factors that may explain the low number of prosecutions over the evaluation period.

265. One important reason relates to a constitutional challenge through 121 petitions to PMLA provisions since 2018, which put on hold a number of trials and was only disposed of by the Supreme Court (*Vijay Madanlal Chowdhary vs. Union of India*) in July 2022.

266. The challenges were made to several powers of the ED under the PMLA that would have impacted their investigations and prosecutions over the period. These included challenges to the scope of the ML offence, the power to provisionally attach property without a predicate offence being registered, the status of such attachment after 365 days, ED's search and seizure powers, the civil burden of proof, bail conditions, protection against self-incrimination, the requirement to record an Enforcement Case Information Report (ECIR), the standalone nature of ML, amongst others. These challenges also impeded trials in other ML cases as the Courts adjourned these cases pending the outcome of the challenges in the Supreme Court. The issues under challenge were ultimately decided in favour of ED and the provisions of PMLA were upheld. Although there are still legal challenges relating to the PMLA which are waiting decision in the Supreme Court, this has not impacted PMLA prosecutions since the 2022 decision.

267. Following the decision by the Supreme Court in 2022, prosecutions that had been stalled by the legal challenges have all resumed. However, there were a significant number of ML cases that could not be prosecuted during this period. The courts have taken several initiatives to fast-track trials since 2022, such as courts cutting shorter dates for sessions, using video conferencing facilities for suspects and witnesses, and the use of remote points for video conferencing in Indian Embassies and Consulates around the world. Although the number of ML prosecutions and convictions have started to increase over the period of 2022-23, as reflected by the statistics, the backlog remains considerable.

268. The limited number of specialised ML prosecutors in ED and judges of Special Courts has also contributed to a saturation of the judicial system i.e., inability to prosecute additional cases due

[89] The data pertains to financial year i.e., from 1st April to 31st March.

to reaching prosecutors and courts' full capacity. The authorities recognise the importance of addressing the shortage in human resourcing and have plans to address this partly through increases to the number of ED prosecutors from 173 to 300 over the coming years.

269. Finally, Indian authorities also noted that an additional 171 prosecution complaints are not progressing on account of pending international assistance based on requests made by India.



### Table 3.13. ML Prosecution Complaints (PCs) by Underlying Predicate Offence

| Predicate crime type | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022- Oct 23 | Total |
|---|---|---|---|---|---|---|
| Fraud and forgery | 177 | 52 | 137 | 124 | 340 | 830 |
| Convictions | 0 | 0 | 1 | 1 | 12 | **14** |
| Corruption and bribery | 87 | 41 | 54 | 52 | 144 | 378 |
| Convictions | 0 | 1 | 0 | 2 | 7 | **10** |
| Illicit arms trafficking | 12 | 6 | 9 | 7 | 16 | 50 |
| Convictions | 1 | 0 | 0 | 0 | 0 | **1** |
| Terrorism, including TF | 11 | 0 | 12 | 2 | 15 | 40 |
| Convictions | 0 | 3 | 0 | 0 | 4 | **7** |
| Illicit trafficking in narcotics | 3 | 2 | 5 | 9 | 8 | 27 |
| Convictions | 5 | 0 | 0 | 0 | 0 | **5** |
| Murder, grievous bodily injury | 7 | 2 | 4 | 1 | 6 | 20 |
| Convictions | 0 | 1 | 0 | 0 | 0 | **1** |
| Smuggling | 2 | 0 | 3 | 3 | 12 | 20 |
| Extortion | 4 | 1 | 4 | 1 | 10 | 20 |
| Environmental crime | 2 | 2 | 1 | 2 | 7 | 14 |
| Convictions | 0 | 1 | 0 | 0 | 0 | **1** |
| Illicit trafficking in stolen and other goods | 1 | 0 | 3 | 0 | 6 | 10 |
| Robbery, theft | 1 | 0 | 1 | 0 | 5 | 7 |
| Piracy of products | 0 | 0 | 1 | 0 | 4 | 5 |
| Human trafficking and Migrant Smuggling | 0 | 0 | 1 | 2 | 2 | 5 |
| Sexual exploitation, including of children | 1 | 0 | 0 | 0 | 0 | 1 |
| Tax crime under Black Money Act | 1 | 1 | 1 | 1 | 2 | 6 |
| Convictions | 1 | 0 | 0 | 0 | 0 | **1** |
| Counterfeiting currency | 1 | 0 | 1 | 0 | 0 | 2 |
| Insider trading | 0 | 0 | 0 | 0 | 1 | 1 |
| **Total** | **310** | **107** | **237** | **204** | **578** | **1436 PCs** |

N.B. Each PC may comprise multiple categories of offences.

## *Types of ML cases pursued*

270. Based on cases provided, the assessment team noted that the ED was able to pursue different types of ML cases, including complex and large-scale cases, involving various ML typologies, such as TBML, third party ML, hawala and cash couriers, and ML related to foreign predicate offending. During the period under review, ML investigations in thirteen cases have been carried out in relation to foreign predicate offending, resulting in five prosecution complaints.

271. India has provided data reflecting significant numbers of ML cases involving stand alone and third-party laundering (Table 3.14 and 3.15). The PMLA does not require that there also be a conviction or even an investigation of the associated predicate offence, and there have been several cases where ED has initiated investigation of ML irrespective of an investigation of the predicate crime. In many cases, ED has done this by focusing on tracing of the proceeds of crime and the illicit manner in which the proceeds are concealed and layered.

### Table 3.14. ML Investigations by typologies

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (until Oct) |
|---|---|---|---|---|---|---|
| ML investigations involving natural persons | 195 | 562 | 981 | 1180 | 949 | 296 |
| ML investigations involving legal persons | 158 | 285 | 808 | 876 | 743 | 251 |
| Standalone ML investigations | 35 | 84 | 127 | 129 | 118 | 62 |
| Third Party ML investigations | 119 | 411 | 667 | 765 | 626 | 219 |

### Box 3.13. Stand Alone ML Case

ED recorded a case based on FIR registered by police for predicate offences of cheating (fraud) and criminal conspiracy under the IPC, 1860.

Accused A and his associates B and C had cheated various suppliers by issuing post-dated cheques for the goods supplied by them, which when presented before the respective banks were dishonoured. The accused sold the purchased goods in the market and did not pay back the supplier's dues, thereby cheating the suppliers. Based on complaints from various Suppliers, seven FIRs were registered against the accused.

ED traced and attached three immovable properties of the accused worth 7.1 million INR (EUR 79 000). A Prosecution Complaint u/s.45 of the PMLA, 2002 was filed before the PMLA Court against 5 accused persons includingf A, Band C .

Though the accused were acquitted in the triall for the predicate offence, they were convicted in the PMLA case.

The PMLA Court passed an order convicting Mr. A and three others for the offence of Money Laundering and sentenced them to imprisonment for three years and imposed a fine of INR 5 000 (EUR 55.85) for each of the four accused. The Court also ordered confiscation of the Properties attached by ED. One of the accused, Mr. D passed away during the trial.

272. Although 1 359 legal persons have been prosecuted over the evaluation period, only three legal persons have been convicted which is relatively low considering the significant number of cases involving legal persons presented in the case studies, although the challenges in securing convictions for legal persons are similar to those for natural persons over the review period (as explained above).

### Table 3.15. ML Prosecution by crime type

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022- Oct 23 | Total |
|---|---|---|---|---|---|---|
| Nos of prosecutions | 216 | 51 | 130 | 144 | 323 | 864 |
| No. of persons prosecuted for Self-laundering | 183 | 232 | 168 | 124 | 431 | 1615 |
| 28 Convictions over this period | | | | | | |
| No. of persons prosecuted for Third Party laundering | 70 | 289 | 656 | 173 | 561 | 1 749 |
| 17 Convictions over this period | | | | | | |

## *Effectiveness, proportionality and dissuasiveness of sanctions*

273. Between 2018 to the date of the onsite visit, ED has been able to secure conviction in 28 ML cases involving 56 natural persons and three legal persons. The Indian authorities provided the table below that reflects sentences imposed for ML which are broadly effective, proportionate and dissuasive.

### Table 3.16. Sentencing for ML

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022- Oct 23 | Total |
|---|---|---|---|---|---|---|
| 0 – 2 years | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 – 4 years | 1 | 5 | 0 | 2 | 25 | 33 |
| >4 years | 7 | 2 | 1 | 2 | 11 | 23 |

274. In addition to imprisonment, the PMLA also provides for fines which are without any limit and are ordered by the Special Court in proportion to the nature and extent of offence committed, allowing for a proportionate approach for lesser sentences and helping to add to the dissuasiveness of more severe ones. The average length of custodial sentences imposed for ML convictions is 4.8 years ranging from 3 years to 7 years and average fine imposed for ML convictions is INR 1.05 million (EUR 11 515) ranging from INR 5,000 (EUR 55) to INR 20 million (EUR 219 300).

275. There is no formula for sentencing (i.e., the judge must apply their judgement according to the particular facts of the case in question) nor is there any formal guidance for judges that would establish factors determining the severity of the penalty. However, case law provides some general principles such as that higher punishments have been awarded to the main accused and lesser to the accused who assisted in money laundering, in accordance with proportionality.

276. Based on case studies presented, the Courts have not hesitated to pass relatively dissuasive sentences of seven years imprisonment. There have been no repeat offenders. Prosecution may appeal acquittals and unsatisfactory sanctions; however, this has not been done in practice. There have been three cases where fines have been imposed upon legal persons for convictions, of INR 50 000 (EUR 560), INR 100 000 (EUR 1 120) and INR 500 000 (EUR 5 600). In addition, property representing proceeds of crime of legal person has also been confiscated.

## *Use of alternative measures*

277. In cases where a trial for ML cannot be completed and it is not possible to secure a ML conviction for any particular reason, India's response is largely to aggressively pursue the assets of the launderer under the broad provisional attachment powers under the PMLA, as well as under other legislation such as the Fugitive Economic Offenders Act (2018) and the Benami Transactions (Prohibition) Amendment Act (2016) (See IO.8).

278. Indian authorities have also used provisions under the Income Tax Act to apply punitive tax measures (83.25% tax) against unexplained wealth and assets. This has been mainly used against persons holding assets from undisclosed sources as well as hawala operators.

3

### Box 3.14. Income Tax Measures

Investigations through search and seizure action in 2020 under the Income Tax Act revealed that ABC and his associates were part of an illegal syndicate involved in providing dummy accommodation entities for the purpose of operating hawaladars and for ML. Documentary and digital data showed that money was moved between multiple dummy Indian entities controlled by ABC (based in India), and foreign entities controlled by foreign associates. These dummy entities were also used to launder undisclosed income. Penal proceedings against ABC under sections 276C, 277 and 278 of the Income Tax Act and sections 420, 468, 204, 120B of the Indian Penal Code have been initiated. These involved tax evasion, false returns of assets outside India, cheating and fraud.

## Overall conclusion on IO.7

India pursues a systematic approach to identification and investigation of ML cases, making use of a range of different avenues to initiate cases. ED's governance framework in identifying and selecting ML cases for investigation is well established through risk-informed Technical Circulars.

The proportion of ML cases identified, investigated and prosecuted appears to broadly reflect the risk profile of India. ED investigators are well trained for and are able to use a variety of investigative skills to trace complex money trails. The ED has the capability to investigate and prosecute different types of ML cases, involving various ML typologies, such as TBML, third party ML, and foreign predicate offending.

Although the number of ML investigations increased since the review period the number of prosecution complaints and concluded trials had not caught up accordingly. This is attributed to a constitutional challenge of PMLA provisions and concerns of limited number of prosecutors and lower number Special Courts and judges specialised in ML cases with apparent saturation in the judiciary. This has a significant impact on India's ability to ensure that offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions, and is therefore weighted significantly. It is critical India addresses these issues in view of accused persons waiting for cases to be tried and prosecutions to be concluded.

India is rated as having a moderate level of effectiveness for IO.7.

## Immediate Outcome 8 (Confiscation)

### *Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective*

279. India has a long-standing national policy priority on confiscation and has strengthened its focus on asset recovery since its last MER in 2010. This has been demonstrated through India's promotion of asset recovery internationally as part of its G20 presidency, the implementation of processes and operational objectives of LEAs, and through the series of legislative amendments over the past decade that have given competent authorities broad powers to freeze and confiscate assets in broad circumstances.

280. India has currently established its national policy objectives for the attachment (seizure), confiscation and recovery of proceeds of crime domestically and internationally as set out in India's National AML/CFT/CFP Policy Action Plan and Strategy Statement 2023-2028. The National Strategy contains a standalone objective on strengthening asset recovery procedures, with three high-level action points for the Enforcement Directorate (ED) under this overarching objective. These are streamlining procedures for seizure and confiscation; ensuring the rapid disposal of pending cases by special courts; and improving the recovery of proceeds outside of India respectively.

281. India has made use of the various coordination mechanisms supporting the competent authorities to share operational information and coordinate cases in view of its enhanced AML/CFT policies, including policy measures to improve confiscation outcomes. New legislation was enacted in the form of the Fugitive Economic Offenders Act (FEOA) in 2018, in order to respond to challenges in recovering proceeds of crime that have moved abroad where the alleged offender has also absconded from the country. ED made policy proposals which were developed by the MAC platform, resulting in additional powers to pursue and recover criminal proceeds on a non-conviction-based basis. How these coordination mechanisms interact with the high-level actions set out for the ED in the Strategy Statement for 2023-2028, and how performance will be measured against specific targets, has not been documented.

282. There is a focus on attachment and confiscation embedded in the PMLA, India's overarching legislation for AML/CFT. Powers to pursue criminal assets have been developed under the PMLA in line with the development of ML risks and policy priorities. Amendments to the PMLA in 2018 and 2019 were made to enhance the powers of ED for attachment (seizure) by increasing the length of time by which assets can be attached prior to the filing of a prosecution complaint and expanding the definition of 'proceeds of crime' to include property of equivalent value held overseas. These amendments were proposed by the Ministry of Finance with the input of the ED and other stakeholders who had identified the gap in application of the PMLA at the time.

283. However, various powers under the PMLA have been subject to challenges in the Supreme Court, with a recent ruling in July 2022 finding this regime to be constitutional (see Chapter 1 and IO.7). During the period of challenge, ML cases did not progress through the courts for finalisation of proceedings which has impacted the ability of Indian authorities to make further legislative changes or meet other ML operational objectives.

284. Other legislation has also been enacted in support of India's national policy on the confiscation of proceeds of crime, with many of these amendments in response to the recommendations of the White Paper on Black Money (2012) Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015; Benami Transaction (Prohibition) Act, 1988 as amended in 2016. (See Chapter 2).

285. At an agency level, depriving criminals of the proceeds of their crimes is prioritised as part of the objectives of agencies, resulting in identification of potential proceeds of crime at the onset of an investigation and swift action to seize these proceeds. Law enforcement agencies at the State level identify assets for attachment and confiscation in all proceeds-generating cases and this is included as a mandatory field in the filing of an FIR and in charge sheets. Training is provided to the economic offences wing of State LEAs to enable them to identify and seize assets which helps to embed a focus on attachment and confiscation in all investigations of proceeds-generating offences.

286. The ED retains statistics on ML attachments and confiscations that may help inform operational and policy decisions. At the State and District Levels, statistics on seized property is maintained by the relevant Competent Authority and Adjudicator (CAA) or police station, but comprehensive data on post-conviction orders and ultimate confiscations are not centrally maintained or integrated with CCTNS. This impacts India's capacity to readily have a comprehensive and coordinated picture on the effectiveness of its confiscation regime at all levels in the country.

### *Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad*

287. The ED has a broad set of measures for depriving criminals from the benefits of their crimes through the attachment (seizure) and confiscation of proceeds and instrumentalities of crime in accordance with the PMLA. Complementing the PMLA, the powers in the Indian Criminal Procedure Code (CrPC), FEOA (and seizure/confiscation powers under other legislation focused on the specific types of offences, such as the UAPA, Customs Act, NDPS Act and Arms Act) provide other LEAs both at the central and state level with the powers to identify, attach and ultimately confiscate proceeds of crime (see. R.4).

#### *Enforcement Directorate - Provisional measures*

288. The ED has primary responsibility for ML investigations and pursues seizure through the attachment of assets. ED officers receive thorough training in financial investigations that enables them to identify and seize assets. The ED often benefits from the preliminary investigations undertaken by other LEAs for the predicate offence for these purposes.

289. The ED is empowered under the PMLA and guided through its various Technical Circulars, to attach (seize) proceeds of crime at the commencement of all money laundering investigations through the issuance of a provisional attachment order (PAO) in order to prevent dissipation of assets. PAOs are issued against property identified as the proceeds of crime through the ML investigation (see R.4). Under the PMLA, ED can take possession, and administers and manages this property for up to six months, before which time the PAO must be confirmed by the Adjudicating Authority. ED officers are able to attach assets as soon as they have reason to believe the assets may be dissipated if they were to remain in the possession of the alleged offender and this is done in a timely and routine manner.

290. PAOs are heard and confirmed by a quasi-judicial authority, or 'Adjudicating Authority', which consists of three persons with experience in law, finance or administration, who are appointed by the Central Government for a period of five years, as established in Sections 6-8 of the PMLA. As set out in the PMLA, the decision to confirm a PAO is to be taken within 180 days of the ED officer issuing the PAO, with most confirmed within 120-160 days. Upon confirmation of the PAO by the Adjudicating Authority, control over the property, instrumentalities or property of equivalent value continues to be held by the ED. The ED can hold these assets for up to 365 days before a prosecution complaint must be filed and for the entirety of the court proceedings in relation to that prosecution. During this time, the ED effectively manages these seized assets so as

to retain their value until such a time as a confiscation is confirmed subsequent to a conviction, there is court decision to restitute victims or proceed with non-conviction based confiscation is made.

291. As per Table 3.17 below, almost all PAOs issued by the ED were confirmed by the Adjudicating Authority (1 094 of 1 119). The Adjudicating Authority is not bound by the Code of Civil Procedure, but guided by the principles of natural justice and is empowered to regulate its own procedures when considering PAOs. In determining whether the identified properties are involved in money laundering, the Adjudicating Authority considers information provided by the alleged offender as to legitimate sources of income or assets used to acquire the property in question. The onus of proof is on the accused to prove the property was legitimately obtained, with S.24 of the PMLA stating that the presumption of the Authority is that proceeds are involved in ML unless the contrary is proven.

292. As outlined above, the ED identifies assets that may be subject to confiscation in the course of their ML investigation in addition to those already attached by the LEA as part of the investigation into the predicate offence. The ED is also required to initiate an ML investigation and pursue assets if alerted from another source, such as a complaint from the public or by the director of the ED (see Immediate Outcome 7). Technical Circulars have been issued to ensure operational coordination between LEAs and the ED and to prevent the attachment of assets already seized by LEAs.

293. The total value of proceeds related to ML investigations attached (seized) by ED was INR 834.13 billion (EUR 9.27 billion) over the five-year period between 2018 and 2023. This extends to instrumentalities of crime and property of equivalent value. The value of the average PAO is (INR 762.4 million or EUR 8.5 million), although some of the very large cases are likely to have pushed up the average (see Mallya case for example below in Box 3.15).

294. The routine manner in which ED attaches assets at an early stage of investigations is a significant strength of the system, as it substantially reduces the risk of asset flight and also acts as a deterrent. Multiple PAOs may be issued during the course of an investigation as assets are identified and traced, particularly for complex cases involving misuse of corporate vehicles and multiple jurisdictions. ED often relies on its own access to databases, international cooperation (both formal and informal), powers under the PMLA to obtain information directly from REs, and requests for assistance from the FIU-IND to a lesser extent (see IO.6) for identification and tracing purposes. PAOs are issued by the ED to secure assets regardless of whether the confiscation is to ultimately occur after conviction or on a non-conviction basis.

**Table 3.17. ED Attachments and Confiscation (Proceeds and Instrumentalities)**

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022- October 23 |
|---|---|---|---|---|---|
| **PAOs issued** Number | 170 | 167 | 160 | 232 | 390 |
| Value (INR million) | 143 028 | 273 680 | 111 966 | 159 635 | 226 828 |
| Average | 841.3 | 1638.8 | 699.8 | 688.1 | 594.5 |
| **PAOs confirmed** Number | 161 | 161 | 152 | 230 | 390 |
| Value (INR million) | 128 273 | 258 376 | 108 246 | 159 601 | 179 629 |
| Average | 796.7 | 1 604.8 | 712.1 | 693.9 | 460.6 |
| **Confiscation** Number | 4 | 6 | 2 | 7 | 21 |
| Total Value Confiscated (INR million) | 1 104.3 | 231.8 | 4 345.4 | 1 543 14.6 | 15 374.4 |
| Value Confiscated (EUR million) | 12.3 | 2.6 | 48.6 | 1724.2 | 73.6 |

*Enforcement Directorate – Confiscation*

295. Confiscation is undertaken under the PMLA following a finding by the Special Court that ML has occurred and the property is the proceeds of crime. Property that is subject to confiscation by the ED has almost always already been within its possession further to the attachment process as above, and realisation of confiscated assets can occur swiftly after the conviction. This confiscation includes criminal proceeds, instrumentalities and property of corresponding value where the direct proceeds cannot be traced, particularly where the proceeds themselves have been moved overseas. As detailed in Table 3.18 below, conviction-based confiscations of INR 393.7 million (EUR 4.4 million) were executed during the period under review.

296. Approximately 20% of all assets seized have ultimately been confiscated by the ED, both on a conviction and non-conviction basis, with 0.05% of seized assets ultimately confiscated following a conviction and 19.7% of seized assets confiscated on a non-conviction basis. On average, ED completes four confiscations each year with an average INR 17.2 million (EUR 191 000) per confiscation following a conviction, and three confiscations with an average INR 9.7 billion (EUR 107.8 million) confiscated each year on a non-conviction basis. Challenges in securing confiscations on the basis of a conviction under the PMLA have largely been due to the impact of the claims before the Supreme Court on provisions within the PMLA on the conclusion of prosecutions before the special courts, during which time the attached assets remain under the control of the ED. As per Table 3.18 below, the number of conviction-based confiscations slowed between 2020 and 2022 during this challenge. Following the decision of the Supreme Court, authorities were able to continue with prosecutions resulting in an increase in both the number and value of conviction-based confiscations after 2022. However, the backlog of cases is considerable and will require additional resourcing for these cases to be concluded (see IO.7). Where assets have already been seized, the provisions of the PMLA provide that these assets remain seized during the pendency of the court proceedings, thus helping prevent the risk of dissipation of the assets, with the only provision to seek to retain control of these assets available at the time of consideration of the PAO by the Adjudicating Authority.

297. There are also provisions within the PMLA where non-conviction-based confiscation can occur when a trial cannot be conducted or concluded. An application can be made by the Director of ED or any person entitled to the attached property (such as a victim of crime) and the Special Court may then order the confiscation or release of the property. The burden of proof requirement under the PMLA is on the accused. Non-conviction-based confiscation may also take place under the FEOA in the circumstances whereby an individual has fled India and has been declared a fugitive economic offender (See R.4 analysis). This may result in the confiscation of any other assets of an individual suspected of a predicate offence or ML (although this specific legal provision allowing confiscation of any other assets of an individual not linked to or beyond the equivalent value of the processes of crime was not utilised during the review period).

298. The spike in confiscations in 2021-22 is attributable to a large-scale ML case involving INR 141.3 billion (EUR 1.57 billion) (see case study 3.15 below). This case spanned several years and involved multiple lines of enquiry both domestically and internationally. The alleged offender has fled India and is yet to be extradited to face court in India. Proceeds were confiscated on a non-conviction basis under the PMLA and restituted to the bank consortium as victims of the underlying predicate offence (fraud).

### Box 3.15. Case Study: Proceeds laundered from multiple frauds (Vijay Mallya case)

Several reports were filed against Vijay Mallya and others in 2015 and 2016 where it was alleged that a criminal conspiracy existed to cheat (commit fraud) a bank-led consortium in relation to fraudulently obtained loans. Some of these allegedly improperly obtained loans were siphoned off within India and overseas through shell companies and converted into real estate and other assets. Proceeds of crime to the value of INR 112.9 billion (EUR 1.25 billion) were identified by the ED of which INR 50.4 billion (EUR 560.3 million) was seized through two provisional attachment orders in 2016. That same year, Mallya was declared a proclaimed offender due to having absconded from India. Properties owned by Mallya to the value of INR 16.9 billion (EUR 188 million) were also attached under S.83 of CrPC without requiring a proven link to predicate offending.

The ED issued 21 Egmont requests and Letters Rogatory to 8 countries between 2016 and 2020 to identify property and other assets belonging to Mallya. These have resulted in a number of seizures, including a property in France worth EUR 1.6 million, and other assets located in India and abroad.

Mallya has yet to face trial in India and was declared a Fugitive Economic Offender in 2019. His extradition from the UK was approved in 2019 but he is yet to be extradited to India, due to a number of ongoing court processes in the UK.

The bank consortium which had lost money as a result of the fraudulent loans filed an application under the PMLA for restoration of the properties attached by ED. In 2021, the Special Court ordered INR 141.3 billion (EUR 1.57 billion) of moveable and immoveable property be restituted to the consortium prior to the completion of a criminal case. This property was 25 per cent higher than the value of proceeds of crime identified and included interest earned while the property was under the control of the Indian Central Government and returned to the consortium and not into government revenue.

299. For the ED, almost the entire value of confiscations (99 per cent) is the result of non-conviction-based confiscation (NCBC) proceedings, as detailed in Table 3.18 below, the vast majority of which has been restituted to victims. These are largely undertaken utilising the provisions of the FEOA where the suspect has fled the country (five cases during the review period)

and S. 8(7) of PMLA, where a trial cannot be concluded due to the death of the accused, the declaration of the accused as a proclaimed offender, or any other reason as determined by the court (see analysis in R.4), which has been used in 12 cases during the review period, including the significant case referenced above. The other cases where confiscation occurred on a non-conviction basis relate to alleged fraud, corruption, drug trafficking, TF and human trafficking.

300. There is a focus on using these provisions to provide restitution to victims of crime, particularly where these have been state-owned banks, and to overcome some of the challenges in having alleged offenders extradited to India (see IO.2). As noted in IO.7, Indian authorities have also used provisions under the Income Tax Act to apply punitive tax measures against unexplained wealth (83.25% tax).

### Table 3.18. Conviction Based and Non-Conviction-based Confiscation for ML

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022- October 23 | TOTAL |
|---|---|---|---|---|---|---|
| **Conviction-based confiscation** | | | | | | |
| Number | 3 | 5 | 0 | 2 | 13 | 23 |
| Value (INR million) | 41.2 | 231.3 | 0.0 | 23.8 | 7.4 | 393.7 |
| Average | 13.7 | 46.3 | 0 | 11.9 | 7.5 | 17.1 |
| **Non-conviction-based confiscation** | | | | | | |
| Number | 1 | 1 | 2 | 5 | 8 | 17 |
| Value (INR million) | 1 063.1 | 0.6 | 4 345.4 | 154 290.8 | 5 277 | 164 976.9 |
| Average | 1 063.1 | 0.6 | 2 172.7 | 30 858.2 | 659.6 | 9704.5 |
| TOTAL (INR million) | 1 104.3 | 231.9 | 4 345.4 | 154 314.6 | 5 374.4 | 165 370.6 |

*Other LEAs and State Police – Seizure and Confiscation*

301. For domestic predicate offences, seizures and confiscations are conducted by several different law enforcement agencies at the central, state and district levels (see R.31). These agencies are responsible for the enforcement of various pieces of legislation concerning fraud, corruption, drug trafficking and general criminal behaviour, such as the UAPA, Customs Act, IPC, NDPS Act and Arms Act. Officers in these agencies are empowered under these laws, as well as the broad powers to search and seize under the CrPC, to identify, trace and seize the proceeds of crime, and have received training to enable them to do so in less complex cases and with limited tracing. Under the CrPC, seized property is held by the police station Officer-in-Charge as case property for offences under the IPC and other Acts until a decision is made by the Magistrate's Court. For offences under the NDPS, a seizure order is provided to the Competent Authority and Adjudicator (CAA) who manages the property and decides on the order within 30 days. Confiscations are executed upon the finalisation of the court proceedings and the securing of a conviction. Nodal officers within these agencies are also required to refer these cases to the ED for subsequent ML investigation (see IO.7) and any corresponding seizure or confiscation would then be undertaken by the ED.

302. As per Table 3.19, LEAs confiscated proceeds of crime and instrumentalities to the value of INR 307.14 billion (EUR 3.41 billion) for the period under review. These figures include all property confiscated, both the proceeds and instrumentalities of crime, including small amounts, but not the proceeds that were pursued as money laundering cases by the ED. As seizures are made across a number of agencies at each level and under various pieces of legislation, comprehensive statistics on attachments for all predicate offences is not routinely collected. While these figures are

significant, it is possible that a portion relate to confiscated assets outside the scope of R.4, and a detailed breakdown is not available. However, authorities provided sample data on the instrumentalities of crime attached and confiscated in India held by one CAA, demonstrating the focus on seizing all assets which may be subject to confiscation. Figures could not be compiled for all CAAs.



### Table 3.19. LEAs and State Police: Confiscations of proceeds and instrumentalities for predicate offences

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-Oct 2023[90] | TOTAL (INR million) | TOTAL (EUR million) |
|---|---|---|---|---|---|---|---|
| Fraud | 3 752.69 | 6 115.6 | 4 189.9 | 923.4 | - | **14,982** | **166.5** |
| Robbery and Theft | 1 4516 | 1 1850 | 1 5610 | 1 8825 | - | **60 801.0** | **675.6** |
| Duty Evasion | 38 628.3 | 114 836.7 | 29 457.1 | 13 237.7 | 31 542.9 | **227 702.7** | **2 530** |
| Criminal Conspiracy | 102.62 | 161.78 | 174.93 | 180.97 | - | **620.3** | **6.9** |
| Drug Trafficking | - | 705.6 | 2265 | - | 2.9 | **2 973.5** | **33.0** |
| Corruption | - | - | - | - | 59 | **59.0** | **0.7** |
| **TOTAL (INR million)** | **56 999.6** | **133 669.7** | **51 696.9** | **3 3167.1** | **31 604.8** | **307 138.1** | **3 412.6** |
| **TOTAL (EUR million)** | **633.3** | **1 485.2** | **574.4** | **368.5** | **351.2** | **3 412.6** | |

Note: Excluding Enforcement Directorate

303. Authorities also seek to restitute victims of crime as part of confiscation activities, both conviction and non-conviction based. This occurs particularly in relation to fraud (see Case Study 3.15 above). Examples have been provided by India in this regard. As noted in IO.1, since 2021, more than INR 6 billion (EUR 67 million) has been recovered by I4C through the CFCFRMS portal and returned to victims of cyber-enabled fraud, in addition to the fraud-related figures in Table 3.19 above. These funds are able to be returned to victims quite quickly as detailed in Case Study 3.16 below.

[90] Statistics were not provided for period 2022 to 2023 for fraud, robbery and theft, and criminal conspiracy.

### Box 3.16. Case Study: Use of CFCFRMS portal to restitute victims of cyber-enabled fraud

Mr AAB of Gujarat reported a loss of INR 103,764 (EUR 1,153) to CFCFRMS on 30 March 2023 as a result of four unauthorised debit transactions from his State Bank of India (SBI) account. This money was taken out of his SBI account and transferred to PayTM and Yes Bank (two other FIs). Upon receiving the report, the funds were frozen by PayTM that same day, amounting to INR 99,764 (EUR 1 108). On 31 March 2023, this amount was refunded by the police in collaboration with PayTM to Mr AAB.

*Asset Management*

304. India has mechanisms in place to manage seized assets and ensure they retain their value until confiscation occurs, following the completion of the judicial process or NCBC. At the state and district levels, this is primarily achieved through the CAAs located in four metropolitan cities (Delhi, Kolkata, Mumbai and Chennai), or via local police stations. The assets managed by these CAAs are generally moveable property seized during the course of predicate offence investigations, including low level offending. These CAAs do not manage more complex assets and capacity of these four CAAs to service the entirety of state and district LEAs, in addition to local police stations, may not be sufficient.

305. At the central level, ED manages all assets seized and confiscated by it. Processes and procedures for managing moveable and immoveable assets, as well as intangible property, such as patents and virtual assets, are in place, with greater capacity and capability at the central level. ED has effectively managed these assets to ensure they retain their value, including the management of shares as part of the Mallya case (Box 3.15 above) as well as cryptocurrencies as per Box 3.17 below. As noted above, ED maintains comprehensive statistics at the central level on confiscated assets, but there is no centralised repository for data held by each of the CAAs and LEAs on assets seized and confiscated.

### Box 3.17. Case Study: Management of seized virtual assets

As part of an investigation relating to fraud via an online gaming app, the ED traced proceeds of crime to a number of cryptocurrencies and tokens. These virtual assets, valued at INR 144.7 million (EUR 5 million), were seized by the ED and secured in a cryptocurrency wallet opened in the name of ED. An application was then put before the Special PMLA Court to convert the cryptocurrency to fiat currency to mitigate the risk of depreciation of value on the basis of expert consultation on the matter. The Special PMLA Court asked the concerned party to convey its consent to the conversion or otherwise within two weeks' time. Upon receipt of this consent, the Special Court allowed the conversion of cryptocurrency to fiat currency and the value of the seized assets secured.

*Foreign proceeds in India, and proceeds abroad*

306. India is generally not considered a destination country for criminals to launder their proceeds generated from foreign predicate offending, although does attract foreign proceeds to some extent (see Chapter 1). Seizure and confiscation of assets based on foreign predicates is largely conducted by the ED in response to MLA requests. Between 2018 and 2023, India received

eight requests from foreign jurisdictions for seizure of assets located in India, of which six have been executed and the available assets attached (see Box 3.18 below).

307. For the period January 2018 to December 2022, the ED also sent 47 requests related to 16 cases to foreign jurisdictions for the recovery of INR 141.33 billion (EUR 1.57 billion), of which 15 requests involving INR 10.79 billion (EUR 119.85 million) have been executed and the assets seized in relation to nine cases. These requests included the Mallya case cited above (case study box 3.15), as well as predicate offences of fraud, corruption, forgery, attempted murder and organ trafficking.

### Box 3.18. Cross-border cases

#### Repatriation of Assets to the United Arab Emirates (UAE)

An MLA request was received during March 2019 from the UAE in connection with fraud to the value of INR 19.87 million (EUR 220 000). The accused had embezzled funds from the Economic Exchange Centre (EEC) and 38 fraudulent transactions made to 32 bank accounts in India, held by 32 individuals. The request sought information on the beneficiaries of these transfers at various banks located in India, and any further transactions from these accounts to other beneficiaries.

The request was executed by law enforcement agencies in India and the details of the beneficiaries in whose accounts the funds were fraudulently transferred were shared with the UAE authorities. These accounts were subsequently searched and frozen in order to recover the proceeds of crime. Seven transactions to the value of INR 3.46 million (EUR 38,000) were immediately repatriated and a further INR 6.18 million (EUR 69 000) subsequently recovered and returned to the EEC in the UAE. A criminal investigation was initiated in India with details shared with counterparts in the UAE.

#### Assets in Hong Kong, China

An ML investigation was launched by the ED in 2019 in relation to suspected fraud and criminal conspiracy to the value of INR 20.4 billion (EUR 226 million). The accused fraudulently embezzled the funds from their company, siphoning the funds through a complex network of 70 legal persons, including shell companies both within India and abroad. During the course of the investigation ED attached assets worth INR 1.9 billion (EUR 20.8 million) in India. An MLA request was sent to Hong Kong, China to seize assets and an insurance policy valued at USD 15 million (EUR 14 million). It was found that the insurance policy had already been surrendered by the policyholder and no funds were available for seizure.

308. India has identified challenges associated with the recovery of assets located overseas, especially in relation to NCBC requests. To overcome these challenges, India also attaches property of corresponding value located in India in the event that assets cannot be repatriated from other countries. Of the requests detailed above, property of equivalent value to the amount of INR 52.65 billion (EUR 585 million) has been attached in India in relation to 16 requests, pending finalisation and confiscation orders.

### *Confiscation of falsely or undeclared cross-border transaction of currency/BNI*

309. India has a system of capital controls under the Foreign Exchange Management Act, 1999 (FEMA), which restricts the flow of Indian and foreign currency entering and leaving India. Strict procedures are in place at sea and airports to screen passengers and their baggage in order to identify undeclared cross-border currency movements. Key borders are fortified with secure

fencing and cross border movements are heavily scrutinised. Cargo and postal systems are also subject to adequate processes for the detection of currency and BNI, mainly using screening, review of documentation and physical inspection on a risk basis.

310. Border agencies, including Customs, Immigration, Air Intelligence Units, Indian Coast Guard, and Postal Authorities coordinate and collaborate at the major ports to share risk information on passenger profiles and conduct joint activities on smuggling investigations. They also coordinate with other relevant agencies such as the FIU-IND and LEAs at state and central levels when additional sources of intelligence or the exercise of powers under other legislation is required. Border agencies are also provided sufficient training on risk profiling for cash couriers.

311. Border agencies use profiling and risk parameters to identify travellers who should be subject to more thorough searches to detect the cross-border movement of cash and BNIs. These risk parameters vary depending on the port of entry/exit and its specific risk profile, such as geographic location, volume of passengers and point of origin for travellers. More stringent processes are in place at the major international airports and seaports which have been identified as higher risk and have been successful in identifying the smuggling of gold.

312. India implements a declaration system for incoming cross border movement of currency and BNIs (see R.32). Travellers are required to complete a Currency Declaration Form (CDF) at all ports when bringing in foreign currency notes exceeding USD 5 000 or when the aggregate value of all forms of foreign currency, including notes and traveller's cheques exceeds USD 10,000. While the focus on Customs' cross-border cash movement detections appears to be more directed towards identifying breaches of the FEMA as opposed to AML/CFT concerns, undeclared cash has been detected nonetheless (see Table 3.21 below). Travellers declaring significant amounts of cash or BNI are not subject to intense questioning or scrutiny if they appear to be carrying cash within their means and the information obtained is not used to trigger broader financial investigations. All cash declarations are provided to FIU-IND on a monthly basis and subject to review by the Strategic Analysis Group. No specific CDFs are flagged by border officials for further intensive analysis by FIU-IND.

313. A disclosure system is in place for outbound passengers and obligations only apply when enquiries are made by Customs officials upon departure from India. Taking more than USD 3 000 out of the country is prohibited, unless the traveller is in possession of a cash memo issued by an authorised dealer, or CDF indicating a higher amount of foreign currency was brought by the traveller into India. No records of disclosures are kept, however, details of all physical inspections of a traveller and their possessions are recorded. It is not clear how regularly these are shared with the FIU-IND or specific instances flagged with FIU-IND, or how outbound carriage of more than USD 3 000 outside, outside of the approval process for issuance of the cash memo is recorded and shared for intelligence purposes.

314. As detailed in Table 3.20 below, India utilised its foreign exchange control mechanisms to seize INR 5.69 billion (EUR 63.18 million) in relation to 2 874 cases of currency falsely declared or in excess of the thresholds under the relevant legislation [FEMA, 1999]. Of this, INR 3.93 billion (EUR 43.68 million) was confiscated, representing a significant proportion (69 per cent) of all cash seized. However, the number of detections appears quite low, given the large volume of air and sea traffic through India. No seizures or confiscation of BNIs occurred during the period under review.

315. Prosecutions were launched in nine percent of cases in which confiscations of currency were made in relation to false declaration provisions under the Customs Act. These do not appear to then translate into further investigations by other LEAs. As per Table 3.20 below, the penalties imposed for these false declarations are dissuasive and effective.

### Table 3.20. Seizure and Confiscation of Cross-Border Movement of Indian and Foreign Currency

| Financial Year | Description of currency seized | Cases in which seizure was done | Value of seizures (INR million) | Cases in which confiscation was done | Value of Confiscations (INR million) | Cases in which prosecution was launched | Penalty imposed (INR million) |
|---|---|---|---|---|---|---|---|
| 2018-19 | Foreign Currency (equivalent in INR) | 710 | 1380.9 | 562 | 975.8 | 43 | 1257 |
| | Indian Currency | 92 | 231.6 | 75 | 174.2 | 7 | 22.4 |
| 2019-20 | Foreign Currency (equivalent in INR) | 600 | 1 192.8 | 542 | 948.8 | 38 | 1 071.5 |
| | Indian Currency | 141 | 184.3 | 117 | 80.9 | 8 | 147.3 |
| 2020-21 | Foreign Currency (equivalent in INR) | 186 | 505.9 | 200 | 714.7 | 26 | 129.3 |
| | Indian Currency | 48 | 62.6 | 41 | 51.1 | 3 | 6.5 |
| 2021-22 | Foreign Currency (equivalent in INR) | 320 | 513.2 | 285 | 395.4 | 49 | 216.5 |
| | Indian Currency | 80 | 56.7 | 71 | 44.3 | 0 | 64.1 |
| 2022-October 23 | Foreign Currency (equivalent in INR) | 557 | 1 376.8 | 361 | 528.6 | 44 | 45.1 |
| | Indian Currency | 140 | 181.7 | 101 | 17.7 | 1 | 0.9 |
| **Total** | | **2 874** | **5 686.60** | **2 355** | **3 931.40** | **219** | **2 960.50** |
| **Total (EUR million)** | | | **63.18** | | **43.68** | | **32.89** |

### *Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities*

316. As detailed in Table 3.21 below, the majority of confiscations by ED, including restitution, were related to higher risk underlying predicate offences of fraud, corruption and drug trafficking. However, there is significant variability in results each year during the period under review, with a spike in confiscations in 2021-22, and confiscation of significant proceeds from corruption-related ML has only recently occurred (77% of confiscations occurred in 2023-24). These figures include both conviction and non-conviction-based confiscations.

### Table 3.21. ED confiscations of proceeds and instrumentalities by underlying predicate (Conviction and Non-Conviction Based Confiscation)

| | 2018-19 (INR million) | 2019-20 (INR million) | 2020-21 (INR million | 2021-22 (INR million) | 2022-October 23 (INR million) | TOTAL (INR million) | TOTAL (EUR million) |
|---|---|---|---|---|---|---|---|
| Fraud | 1 063 | - | 3 365.5 | 154 439.7 | 4 478.7 | 163 147 | 18 012.7 |
| Corruption | - | 223.8 | - | 6.3 | 876.7 | 1 106.8 | 12.3 |
| Drug Trafficking | 7.1 | - | 979.9 | 68.6 | 16.5 | 1072.2 | 11.9 |
| Evasion of Duty | 29.9 | - | - | - | - | 29.9 | 0.3 |
| Environmental Crimes | - | 5.3 | - | - | - | 5.3 | 0.06 |
| Arms Act | 4.2 | - | - | - | - | 4.2 | 0.05 |
| Terrorism and TF | - | 1.3 | - | - | 2.4 | 3.7 | 0.04 |
| Murder | - | 1.5 | - | - | - | 1.5 | 0.02 |
| Human Trafficking | - | - | - | - | 0.08 | 0.083 | 0.001 |
| **TOTAL (INR million)** | **1 104.3** | **231.8** | **4 345.4** | **15 4314.6** | **5 374.4** | **165 370.5** | **1 837.5** |

317. Overall, confiscation figures for corruption and drug trafficking (taking into consideration confiscations by ED as well as LEAs) appear low given they are assessed as being moderate to high risk in the NRA, as do environmental crimes although this may also be due to challenges securing convictions during the period under review. The data only reflects confiscations of ML associate with TF by ED, and TF attachments by NIA (through TF prosecutions and UAPA designations) are more comprehensively reflected in IO.10). However, considering NIA generally refers TF cases to ED for ML investigations where there is a strong component requiring the tracing, seizure and confiscation of assets, the data for ML confiscation by ED for TF cases are quite low given the TF risks present in India.

318. Nevertheless, the figures of provisional measures (seizures) of proceeds and instrumentalities for ML are largely in keeping with the assessment team's understanding of the volume of these crimes in India. ED is maintaining a focus on targeting complex ML schemes in line with the higher risks of fraud, corruption and drug trafficking as identified in the NRA and the objectives set out in the National AML/CFT/CFP Policy Action Plan and Strategy Statement 2023-2028. In addition, ED has continued to undertake ML investigations and utilise the strong provisional measures under the PMLA to seize property despite the impact of the Supreme Court Ruling during the review period on the PMLA, meaning that confiscation results themselves are not consistent with the risks during this period. India has made use of NCBC tools in order to confiscate proceeds in cases under the FEOA and PMLA, confiscating some of the higher proceeds generating crimes where offenders have absconded, consistent with national priorities and a focus on restituting victims of crime.

319. Table 3.22 below provides figures on the overall confiscation figures by all competent authorities. These figures are less relevant when drawing general conclusions on consistency with risk, as the ED has a sophisticated process for identifying and proceeding with ML cases based on risk and national priorities, drawing from the NRA (see IO.7), and therefore represent the most important proceeds generating offences. In addition, the figures include all proceeds generating offences (including those generating small amounts but are frequent in occurrence). Nevertheless, for the period under review, LEAs (other than ED) confiscated INR 14.98 billion (EUR 166.5 million) in relation to 319 cases of fraud, which is one of the highest risk proceeds generating offences.

### Table 3.22. ED and other LEAs Confiscation of proceeds and instrumentalities

| | Predicate agencies | | ED | | | |
|---|---|---|---|---|---|---|
| Offence | TOTAL | TOTAL | TOTAL (ML-linked) | TOTAL (ML-linked) | TOTAL | TOTAL |
| | (INR million) | (EUR million) | (INR million) | (EUR million) | (INR million) | (EUR million) |
| Arms Act | - | - | 4.2 | 0.05 | 4.20 | 0.05 |
| Corruption | 58.90 | 0.7 | 1 106.8 | 12.3 | 1 165.70 | 12.97 |
| Criminal Conspiracy | 620.3 | 6.9 | - | - | 620.30 | 7.07 |
| Drug Trafficking | 2 973.50 | 33.0 | 1 072.2 | 11.9 | 4 045.70 | 44.90 |
| Duty Evasion | 227 702.7 | 2 530.0 | 29.9 | 0.3 | 227 732.6 | 2 530.3 |
| Environmental Crimes | | 0.0 | 5.3 | 0.06 | 5.30 | 0.06 |
| Fraud | 14 982 | 166.5 | 16 3147 | 1 812.74 | 17 8129 | 1 979.2 |
| Human Trafficking | - | 0.0 | 0.083 | 0.001 | 0.08 | 0.00 |
| Murder | - | 0.0 | 1.5 | 0.02 | 1.50 | 0.02 |
| Robbery and Theft | 60 801 | 675.6 | - | - | 60 801.00 | 675.6 |
| Terrorism and TF | - | - | 3.7 | 0.04 | 3.70 | 0.04 |
| **TOTAL** | **307 138.40** | **3 412.65** | **165 370.68** | **1837.41** | **472 509.08** | **5 250.10** |

320. Indian authorities have also sought to recover assets located overseas through informal and formal cooperation mechanisms, largely in keeping with the risk profile. However, as discussed in IO.2, transnational asset seizures for the period under review has been achieved for INR 10.79 billion (EUR 119.85 million) out of a requested INR 141.33 billion (EUR 1.57 billion). As noted above, these have not translated into confiscations which was explained by India as being largely due to foreign jurisdictions' unwillingness to confiscate and repatriate assets to India for NCBCs

## Overall conclusion on IO.8

India's confiscation regime proactively deprives criminals of the proceeds, instrumentalities and their corresponding value for ML and predicate offending through the timely and routine use of provisional measures resulting in a significant quantity of assets being seized and held by India, although ultimate confiscation of proceeds is not in line with the risks due to challenges associated with achieving convictions (see also IO.7). Nevertheless, India's system of seizure has helped prevent the dissipation of proceeds given it occurs at an early stage of an investigation, with the majority of proceeds held by the ED and CAAs while awaiting confiscation orders.

India has a wide range of legislative measures available to help law enforcement in their efforts to identify, seize and confiscate proceeds, and LEAs, especially at the Central Government level, are capable of applying them. This has helped India also secure confiscate proceeds via non-conviction-based confiscation procedures in a number of important cases. This has been weighted heavily as they represent the permanent deprivation of proceeds in some significant cases. Nevertheless, with the resolution of the constitutional challenge under the PMLA, India should focus on pursuing confiscation of criminal proceeds of through more conviction-based confiscations.

India has a system of capital controls, with the focus on cross-border cash movements focused on identifying breaches of these controls as opposed to AML/CFT concerns, with the number of these breaches quite low given the risk and context of India. Outcomes, information-sharing and international cooperation has been implemented for the declaration system for incoming cross-border movements, but to a significantly lesser extent in the disclosure system for outgoing movements.

India is rated as having a substantial level of effectiveness for IO.8.

# Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

## Key Findings and Recommended Actions

## Key Findings

Immediate Outcome 9

a) TF cases with a multi-state and/or cross-border nexus are investigated at the central level by the National Investigative Agency (NIA), and the ML aspect of TF cases is investigated by the Enforcement Department (ED), with links between TF and organised crime in some cases in India. The NIA and ED have skilled and highly experienced investigators and in-house prosecutors to conduct complex financial investigation and identify money trails domestically and abroad, to support the investigation and prosecution of terrorist activity and TF.

b) State Police are empowered to investigate State-wide TF offences, and there are specialised CT authorities at the state level that investigate TF offences. However, the NIA is more appropriately placed to investigate more sophisticated cases of TF.

c) Statistics and case studies reflect significant delays in TF cases being concluded both at the NIA and State level, resulting in a high number of pending cases, so that it could not be concluded that TF offenders were being successfully convicted.

d) Indian authorities have demonstrated a sophisticated understanding of both current and emerging TF threats and risks in different theatres of risk in the country, and investigations and prosecutions are generally conducted in line with the risks identified.

e) TF investigation, operational responses and strategies are closely linked to the country's broader aim of countering domestic terrorism and disrupting domestic terrorist activity, with TF investigations a priority for the country and a pillar of India's national CT strategy.

f) Although fines imposed appear to be relatively small, prison sentences imposed for TF offences, mostly between seven and ten years, provides for a dissuasive sanction, consistent with other serious crimes in India, with the broad range of terms allowing for sentencing according to the gravity of the offence.

Immediate Outcome 10

a) India has in place a legislative framework for the implementation of TFS, through the different forms and layers of communication of updated lists to the reporting entities. These include electronic communication via MEA/MHA and Regulators as well as publication on the websites of the relevant agencies. However, the time and manner in which the obligations to freeze should be implemented is not always clear. While this has limited impact on more established reporting entities that utilise commercial sanction screening software to freeze without delay, the multiple channels and complicated nature of the process has created some confusion for smaller reporting entities, especially some DNFBPs.

b) ITD is responsible for the identification of NPOs operating in India and has utilised a combination of data points from the TF risk assessment to identify "at-risk" NPOs in the country. These data points include the geographical location of NPOs, their function, channels of funding, intelligence information amongst others, to identify a subset of 7 500 NPOs to be at-risk for TF abuse. However, it was not demonstrated that monitoring and outreach prioritised these NPOs.

c) NPOs are required to be registered with and are audited by multiple government authorities on compliance with the different regulations relating to integrity and security, depending on their structure as well as size and source of funds. These varied requirements, sometimes linked to abuse of TF, are not always risk-based or implemented based on consultations with NPOs to avoid negatively impacting their work.

d) There is ongoing engagement with NPOs which is focused on their compliance with different legislations and authorities, as well as the importance of ensuring the legitimacy of the source of funds, the importance of using banking platforms to collect contributions, as well as general TF risks. However, the engagement by the different authorities is not coordinated amongst the different government authorities, and information on specific TF risks relating to NPOs is not adequately communicated. As such, NPOs demonstrated superficial levels of understanding of more specific TF risks relating to their geography or type of activity.

e) India has seized assets from terrorists and terrorist entities through different frameworks. This includes seizures of designated individuals and entities under the UNSCRs, significant amounts from proscribed terrorists under the UAPA, assets from TF investigations (NIA and State Police) and assets from ML investigations related to TF predicate by ED. No TF assets have been confiscated to date.

Immediate Outcome 11

a) Since January 2023, India has in place a framework to implement PF TFS obligations as all natural and legal persons are obligated to freeze funds and assets of sanctioned persons without delay under the WMD Order. UN designations are linked on the MEA website, electronically communicated by MEA to relevant agencies and on FINGATE by FIU-IND, without delay. In addition, there is a communication mechanism that relays listings to

reporting entities through their respective regulators. While it has not been demonstrated that this communication to all REs is taking place without delay, established FIs and VASPs understand their PF TFS obligations and rely on sanction screening software for this.

b) Prior to January 2023, while there was a broad prohibition not to finance sanction persons and entities under the WMD Act and the United Nations (Security Council) Act supplemented by MEA Orders, there was no clear articulation directed at reporting entities on the obligation to freeze funds and assets without delay. UN designations were published on the MEA website without delay and established FIs relied on sanction screening software to implement their PF TFS obligations. However, it has not been demonstrated the extent to which this was done without delay.

c) As part of the onboarding process of the current implementation mechanism, FIU-IND undertook a one-time sanction screening of reporting entities by sending an alert to reporting entities through FINGATE. To date, there have been no matches with designated lists under UNSCR 1718 reported to MEA or FIU-IND through the continuous sanction screening under the WMD Order or generally under the WMD Act, nor the one-time screening process. This appears to be consistent with the limited exposure of India to PF activity.

d) Indian authorities, especially Customs, focus on detecting sanctions evasion techniques, which reduce India's exposure to PF activity.

e) While established FIs and VASPs were aware of their obligations and have the necessary structures (such as sanction screening software) and knowledge to meet their obligations, more recently regulated DNFBPs, do not have the same level of awareness or structures. Although they require more support through clear guidelines, outreach and training, the outreach conducted and inspections by supervisors have been focussed on FIs and significantly less on DNFBPs.

## Recommended Actions

Immediate Outcome 9

a) India should make major changes to address delays relating to the prosecution of TF cases for both natural and legal persons, so as to improve the timeliness of their judicial disposal and clear the serious backlog of current pending cases.

b) India should increase resourcing and enhance the expertise of the CT wings of State Police so that they are able to conduct more sophisticated financial investigations to better support TF investigations, and better placed to support prosecutions at the State level.

c) In order to facilitate effective allocation of resources and clarity of responsibilities, India should articulate in guidelines the circumstances

where TF investigations are referred to the ED for ML investigations.

d) India should formalise and document interagency operational co-ordination and allocation of financial intelligence from FIU-IND on TF to prevent the risk of loss of evidence and intelligence to support TF investigations.

Immediate Outcome 10

a) India should improve its TFS implementation framework so that it is clear that all natural and legal persons are obliged to freeze funds and assets without delay, and streamline the process for communicating TFS listings, in line with the requirements of R.6.

b) Regulators should enhance their outreach and training on TFS obligations, particularly for DNFBPs and ensure that this is regular and sustained.

c) India should ensure that the CFT measures aimed at preventing the NPO sector from being abused for TF are implemented in line with the risk-based approach, including by:

(i) conducting focused outreach to NPOs on their TF risks which should be conducted in a more coordinated and risk-based manner by the relevant competent authorities to ensure that NPOs at risk of TF abuse enhance their understanding of TF risks, including the sources, channels and end-use of funds as per their respective theatre.

(ii) stablishing broad educational or awareness raising programmes (e.g., through social media or other publicity campaigns) to target potential donor communities to sensitise them about their role in avoiding inadvertent support to terrorists or terrorist organisations.

d) NIA should develop its expertise and networks to enable it to better pursue TF assets abroad.

Immediate Outcome 11

a) Regulators should enhance their outreach and training on their PFS obligations, particularly for more recently regulated DNFBPs and less established financial institutions, and ensure that this is regular and sustained.

b) FI regulators should continue to focus on PF TFS in subsequent supervisory cycles and DNFBP regulators should introduce supervision and monitoring of their reporting entities in relation to the implementation of PF TFS obligations.

321. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

## Immediate Outcome 9 (TF investigation and prosecution)

322. TF is criminalised under the Unlawful Activities (Prevention) Act 1967 (UAPA), which is a broad legislative act that provides the authority to respond to activities directed against the integrity and sovereignty of India. While the definition of a terrorist act covers the activity under

the TF Convention, it also encompasses activity beyond the convention. This includes acts with the intent to threaten or likely to threaten the economic security of India, by a list of harmful means which includes "by any other means of whatever nature", acts that disrupt "any supplies or services essential to the life of the community in India or in any foreign country, or acts that "cause damage to the monetary stability of India by way of production or smuggling or circulation of high quality counterfeit India paper currency, coin or of any other material."[91] In relation to this evaluation, the Indian authorities confirmed that the TF cases and statistics for IO.9 and IO.10 that are reflected in the MER, fall within the parameters of Recommendation 5 and acts within the UN TF Convention.



323. As TF is a predicate offence for ML, the ED is able to investigate the ML aspect of TF.

### *Prosecution/conviction of types of TF activity consistent with the country's risk-profile*

324. India has suffered consistently from the impact of terrorism since its independence in 1947. Its authorities demonstrate a sophisticated understanding of the current TF threats in faces, with TF risks predominantly associated with terrorist activity taking place in and around India.

325. Risk assessments identify several sources and channels of funding for terrorism in India depending on the TF theatres (see IO.1). A major source of funding for terrorism for most of the theatres has been linked to sources outside the country. Funding is also identified through the proceeds of various criminal activities such as extortion, trafficking of narcotics and illicit arms generation of funds through businesses and misuse of NPOs; as well as terrorist using their own funds for terrorism. The use of cash couriers and hawala mechanisms present the highest risk in moving funds for terrorism, with banking and card channels as well as Money Transfer Service Schemes (MTSS) and wire transfers less severe but nevertheless present. India is aware of risks posed by FTFs, but these have been small in number in the context of India.

326. The National Investigation Agency (NIA) is the specialised investigating agency under the Ministry of Home Affairs (MHA), that investigates and prosecutes scheduled offences, including TF offences under the UAPA and has concurrent jurisdiction with the State Police on such matters. The Central Government, through the several agencies under the MHA, maintain close liaison with the State Police.

327. Both the National Investigation Agency (NIA) and the Enforcement Directorate (ED) have in-house legal teams that support investigators. NIA has 108 in-house prosecutors who assess the evidence upon the completion of a TF investigation and present the case in court. The ED has 25 legal advisors and 81 legal consultants to support the prosecutors for ED's prosecutions (including for ML) under the PMLA. Based on the cases presented and discussions onsite, NIA and ED prosecutors have sufficient expertise to prosecute TF and ML (with TF predicate) cases respectively. Under the NIA Act, a prosecutor can only be appointed to conduct a trial in the Special Court, courts specifically for terrorism and TF cases (see below), if they have seven years' experience. TF cases for NIA must be assessed by a three-member review body constituted under MHA made up of independent adjudicators with significant legal experience (such as retired judges and legally trained personnel) so that a case can be authorised to proceed for prosecution. This ensures that there is reasonable evidence before prosecution can proceed. A decision is required to be made by the review body within seven days. These factors ensure that TF cases, especially complex TF trials have enough evidence to be taken to court to have charges laid which is the start of the trial process.

328. ED's expertise in dealing with complex financial evidence as well as tracing and seizing assets relating to TF domestically and pursuing assets abroad (as they have the powers to enable

[91] See R.5 (c.5.1).

them to perform this function) is valuable in NIA's pursuit of TF. Between 2018 and 2023, 48 TF cases also have been referred to ED to investigate the ML aspect since TF is a predicate offence for ML. Both agencies maintain strong cooperation and communication, sharing information throughout the investigation of both the ML and TF aspects of the case.

329. India (based on data from NIA and State Police) has initiated prosecutions against 1 530 persons for TF offences between 2018 and October 2023, which is on average about 300 prosecutions a year. For NIA, the data shows that prosecutions were pursued for all suspects investigated for TF and that approximately a third of terrorism cases result in TF investigations and prosecutions. However, for the State Police, although they investigated 60% of TF cases in India, only 28% of TF prosecutions were initiated, suggesting that their CT wings would benefit from enhanced capacity and resourcing.

330. However, while India is prosecuting a reasonable number of cases overall, relative to risks, a small proportion of these cases have resulted in convictions and a high number of pending cases remain outstanding. Between 2018 and October 2023, only cases against 98 persons were concluded, leaving 1432 pending (see table 4.1).

331. Despite having discussed a number of possible explanations with India such as resourcing and processes, it is still not entirely clear to the assessment team why there is such a large number of pending cases. There is a statutory limit from the point in time a suspect is arrested for TF to the point in time charges are preferred (90 days extendable up to 180 days) after which, while waiting for the case to be tried and concluded, the suspect is either allowed bail or remains in remand. The average length of terrorism and TF prosecution is difficult to gauge as it would depend on the number of charges preferred, number of cases heard together as well as the complexity of the case. Based on the charge sheets shared with the assessment team, as a matter of practice, for TF cases, it is usual for NIA to prefer many charges against a suspect after a comprehensive review of each case including whether there was sufficient evidence, which adds to the resources required for the judicial process.

332. The establishment of Special Courts to hear terrorism and TF cases prosecuted by NIA through an amendment to the 2019 NIA Act sought to address this challenge. The Special Court is presided by a judge appointed by the Central Government on the recommendation of the Chief Justice of the High Court. Trials in these courts benefit from the expertise of experienced Judges who have undergone specialised training for example in digital evidence. Fifty Special Courts are in operation in India since 2021. As of October 2023, 120 TF trials were going on in the Special Courts.

333. However, the data reflects that a significant number of TF trials remain unconcluded since 2018, the review period over which statistics have been provided. This is of particular concern, as of the end of the onsite, from the 886 persons whose TF cases being prosecuted by NIA that have not been concluded, 643 remain in judicial custody (126 have died or absconded and 117 have been granted bail).[92] It is therefore critical that these delays are addressed by India while ensuring that due process of the judicial system remains respected. In addition, the number is likely to be larger if cases before 2018 were also factored in.

334. The bottleneck as evident since 2019 appears to be attributed to the long court processes to hear terrorism and TF cases both for cases heard by the Special Courts (despite the increase in number of specialist courts since 2021) as well as TF cases heard at the State level, with frequent and long adjournments built into the trial process. While the COVID-19 pandemic may have had an impact, this does not appear to explain the continuing trend after the pandemic. In addition, no

[92] Due to the seriousness of the offence, bail is not always appropriate, the presumption for bail for TF offences is reversed so that it is automatically refused, with the burden passing to the defendant to show that bail is appropriate.

explanation was put forward in relation to the low number of concluded TF cases for at the state level where the data shows a similar challenge, suggesting similar structural issues that need to be addressed. India noted that there has been significant improvement in the number of concluded cases in the Special Courts over the last two years since, although these have related mostly to terrorism rather than TF prosecutions as the courts have prioritised dealing with terrorism cases rather than TF cases since TF cases are often more complex and take more time.

335. There are plans to provide in legislation, measures to ensure that court cases are concluded in a timely manner. While the complexity of evidence in TF cases invariably means that such cases may take longer to prosecute and the importance of respecting due process, based on the fact that a significant percentage of TF cases consistently remain open across the country over the five-year review period, the assessment team was not able to conclude that TF offenders were being successfully convicted.

### Table 4.1. Numbers of persons prosecuted by NIA and State Police for TF

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (until Oct) | Total |
|---|---|---|---|---|---|---|---|
| NIA | | | | | | | |
| TF Prosecutions | 146 | 170 | 280 | 202 | 143 | 154 | 1 095 |
| Convictions | 5 | 20 | 4 | 9 | 15 | 22 | 75 |
| Acquittals | 0 | 1 | 0 | 1 | 0 | 0 | 2 |
| State Police | | | | | | | |
| TF Prosecutions | 43 | 40 | 28 | 58 | 137 | 129 | 435 |
| Convictions | 4 | 3 | 4 | 2 | 0 | 1 | 14 |
| Acquittals | 2 | 1 | 3 | 1 | 0 | 0 | 7 |
| NIA and State Police | | | | | | | |
| TF Prosecutions | 189 | 210 | 308 | 260 | 280 | 283 | **1530** |
| Concluded cases | 11 | 25 | 11 | 13 | 15 | 23 | **98** |
| Open Cases (net number of open cases per year) | 178 | 185 | 297 | 247 | 265 | 260 | **1 432** |

336. Based on the data provided by India of the TF charges preferred between 2018 and October 2023, most TF prosecutions relate to raising or holding funds for terrorist acts or for terrorist organisations. In terms of proportion of cases prosecuted, approximately two-thirds related to cash couriers or hawala and the remaining were channelled through financial entities such as banks and MTSS, which appears to be broadly in line with the risk profile of the country. This was reflected through the case studies discussed during the onsite. More recently, there has been one case of TF though virtual assets which was investigated by NIA.

337. India provided data reflecting that 419 persons that have been prosecuted for TF related charges under the UAPA involved TF related offences only, without the accused being charged for other the terrorism offences. Case studies were also provided to show how NIA pursued TF prosecutions against independent financial facilitators (See the cases in Box 4.1 and Box 4.4 below).

### Box 4.1. TF involving Maoist activities

In 2020, NIA took over an investigation from State Police where an attack was carried out by a Maoist proscribed terrorist organisation. The organisation was involved in abductions and extortion to fund their activity and also conducted targeted attacks on patrolling police personnel.

Financial investigations, including financial information of suspects from FIU-IND revealed the association of a Mr F who was a partner of a construction firm. Bank account information of the construction firm showed large amounts of assets disproportionate to profits, indicating that Mr F was used the firm to store assets that were to be used to finance the terrorist activity of the proscribed terrorist organisation. The construction firm's bank accounts and other assets amounting to INR 206.5 million (EUR 2.3 million) were frozen.

Mr F was arrested in March 2021 and in April 2021, he was charged with TF charges.

338. Fifty-one legal persons have been prosecuted on TF charges since 2018 by NIA, although none of these cases have been concluded. No legal persons have been prosecuted by the State Police. This is attributed to the same issues as those related to unconcluded prosecutions considered above. Legal entities that face charges include those used in the importation of narcotics or used to hold funds obtained from extortion and other illegal activities, which are subsequently used to fund terrorism, as well as NPOs that are legal entities involved in the support of terrorism and TF.

### *TF identification and investigation*

339. Prior to 2008, TF investigation was solely under the jurisdiction of the respective States' police authorities. However, after the terrorist attacks in Mumbai on 26 November 2008, MHA established the NIA to oversee all TF cases with a multi-state and/or cross-border nexus in order to ensure a more effective response to terrorist activity. Local and non-complex terrorism and TF cases continue to be investigated by the respective State Police.

340. Depending on the threat, different state-specific structures have been set up. For example, the Anti-Terrorism Squad (ATS) was established in the Maharashtra State Police. The ATS receives specialised CT training which includes training in financial investigation, to enable them to target sophisticated organised crime groups that finance terrorist activity in the respective State. Similarly, Jammu and Kashmir has established the State Investigation Agency (SIA) to investigate terrorism and TF cases in the region. Cases may be referred to NIA by the State Police that initiate the investigation (any UAPA offence must be notified to NIA within 24 hours) or NIA may commence investigations on its own accord. Approximately 40% of TF cases in India are investigated by the NIA and 60% by the various State Police authorities.

341. Regardless, NIA understands that state authorities are familiar with state networks and the local languages and thus NIA works in regular close coordination with state authorities on investigations that involve both. NIA provides training and discusses emerging trends and challenges with the State authorities. Based on onsite interviews and case studies, these specialised agencies in the State Police, especially in States where terrorist activity has been present, understand the value of financial investigations related to terrorism. Table 4.2 reflects the number of cases investigated by NIA and the State Police which are generally constant over the review

period. The sudden rise in TF investigations in 2023 is attributed to events arising out of incidents in Manipur that led to TF investigations in over 50 cases.[93]

### Table 4.2. Nos of cases investigated by NIA and State Police for TF

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (until Oct) | Total |
|---|---|---|---|---|---|---|---|
| TF cases investigated (NIA) | 20 | 18 | 26 | 24 | 23 | 24 | 135 |
| TF cases investigated (State Police) | 18 | 19 | 38 | 21 | 23 | 106 | 225 |
| TF cases investigated (Total) | 38 | 37 | 64 | 45 | 46 | 130 | 360 |

342. There is strong interagency cooperation on CT and CFT matters. NIA has a nodal officer in ED since ED also investigates ML where TF is the predicate offence IB (CT/CFT intelligence) and NIA (CT/CFT investigation) also keep communication lines between them open on cases in order to pin-point the optimal point in time to initiate arrests. Whenever State Police open an investigation into an offence under the UAPA, NIA is alerted. Even in cases where a decision is taken that NIA take over a terrorism or TF investigation from the State Police, their practice is to work with the State Police recognising their ground-level connections and language competence.

343. Between 2018 and October 2023, NIA investigated 345 terrorism related cases, which led to 169 charges being filed. NIA investigates the TF element in every terrorism case it investigates, which has resulted in TF specific charges being invoked in 27% of its terrorism investigations. TF investigations have been triggered through various sources including in the course of investigations into terrorism or terror activity, investigations into criminal activity where it is found that the proceeds are used to finance terrorism, and from information coming out of financial or other intelligence, including financial intelligence from STRs that are enhanced with further intelligence and shared by FIU-IND as intelligence packages.

344. Between 2018 and the date of the onsite, FIU-IND disseminated 1 175 TF related STRs to NIA (see IO.6), all of which were analysed. 140 of these were found to be directly related to TF. Based on further analysis by NIA, 26 STRs were directly linked to fifteen TF cases registered in NIA. The remaining STRs, given the absence of clear evidence to initiate investigation, have been retained for further follow-up action. In the same time period, 706 STRs were spontaneously disseminated to the CT wings of the various State Police, of which, 55 were reported to have been found useful. Additionally, 293 STRs were shared by IB with the CT wings of the various State Police and 64 STRs were shared with State Police in response to their requests.

345. STRs not linked to open investigations, are disseminated, simultaneously to IB, NIA and the State Police in order for them to add their own intelligence to the STR and commence researching the intelligence. The matter will then be discussed at the Multi-Agency Centre (MAC) where agencies discuss their findings and for a decision to be made as to whom will be the lead agency. It was not clear how the agencies deconflict with each other prior to the MAC nor reduce the risk of loss of evidence and intelligence. A more streamlined process allocating the STR to a lead agency at the outsight would help to resolve this potential issue as well as allow resources to be deployed on other work.

[93] Each case often results in the prosecution of several suspects, especially where the case involves investigation into a terrorist organisation (which explains why there are more prosecutions than cases investigated).

### Box 4.2. TF Investigation on the basis of STR

In June 2020, NIA received an STR from FIU-IND in respect of Mr A. The STR was filed on the basis of adverse media reports as well as irregular transaction patters where Mr A was operating a business account with only cash withdrawals and no business transactions. Details of his other accounts along with identifiers were also shared in the STR.

The STR led to the initiation of investigation into the business activities of Mr A and others, which led to the uncovering of terrorist financiers who were involved in under-invoicing that created a trade imbalance and generated profits that were used to support the sustenance and operations of terror organisations of the Hizbul Mujahideen and Lashkar-e-Tayyiba. The traders were involved in the generation and distribution of funds for the terrorist organisations although not directly involved in terrorist activity. They are currently facing prosecution for TF charges under the UAPA.

346. Most case studies presented, reflected investigations that were triggered by intelligence on terrorist activity or activity supporting terrorism, through sophisticated surveillance and investigation mechanisms by IB and NIA. They collect and analyse intelligence on terrorist activity and subsequently coordinate action based on the intelligence, especially the decision-making process associated with when a case should move forward for prosecution. NIA has access to a broad range of operational intelligence for both terrorism and TF through various platforms (see IO.1) such as the MAC and Subsidiary MAC (SMAC) platforms for sharing information and intelligence and the Fake Indian Currency Note Coordination Group (FCORD).[94]

347. As TF through proceeds of criminal activity is a risk area in India, the MAC/SMAC platform is useful as it brings together intelligence agencies, FIU-IND and operational agencies involved in TF investigation, as well as those that investigate other organised criminal activity such as drug trafficking that may have a TF connection. The representation of State Police, central agencies, FIU-IND as well as RBI in FCORD also adds to the value of this mechanism due to the financial information and intelligence they contribute to support the identification of TF. Continued emphasis on developing TF investigations based on financial intelligence such as STRs would provide even greater opportunities for investigating agencies to identify and pursue stand-alone TF.

[94] Initially set up to counter fake currency syndicates and has evolved into a group that coordinates and streamlines CT efforts of various agencies in India.

### Box 4.3. TF Investigation resulting from a criminal investigation

In 2019, the State Police of Punjab apprehended suspects found with 500 grams of heroin and INR 120 000 (EUR 1300) in cash in their possession. Investigations were transferred to the State Special Operations Cell of the Punjab State Police, which revealed a network of drug traffickers and hawala conduits as well as the involvement of the proscribed terrorist organisation, the KLF. NIA took over the investigations and it was found that the commander of KLF ran a drug smuggling network to support the organisation and channelled the proceeds of the sale of drugs through hawala operatives for the utilisation of terrorist activity of the KLF. Upon the completion of investigation, 14 suspects have been prosecuted for TF.

348. NIA has significantly increased its resources over the last four years, with 50% more branches and 40% increase in personnel as noted in IO.1. NIA investigating officers are recruited based on their experience, most of whom have at least eight years of field experience and have undergone basic police training. In addition, NIA officers are provided with additional training with a focus on collection of intelligence, including financial intelligence. Similarly State Police, particularly the CT-wings of the State Police, receive basic police training, additional training as per their specialisation, and training in TF investigations by NIA, IB and FIU-IND. NIA has data analysts to assist with their financial investigation. Both NIA and State Police have access to forensic accountants and can recruit private expertise where needed. However, the cases indicate that these are used more regularly by NIA which is consistent with the complexity of cases investigated by NIA as compared to the State Police.

349. NIA and ED have access to a wide range of financial information and intelligence to support their TF investigations (See IO.6). They can obtain bank account information through FIU-IND or directly from banks without the need for a court order. Where more complex financial investigation involving tracing and seizing of property is required for TF, ED is able to initiate a ML investigation (since TF is a predicate offence for ML) to draw upon their resources and expertise and extended seizure powers. NIA and ED will share intelligence or conduct joint investigations by coordinating search and seizure operations or arrests where this will assist in ongoing investigations. Such coordination has occurred 48 times over the assessment period. NIA has direct access to National intelligence Grid (NATGRID), which is an integrated intelligence database for security and CT purposes. Since September 2023, this access has been extended to the State Police. It serves as a valuable intelligence and investigative tool for TF because it contains links to various databases.

350. During the onsite, the assessment team was presented with several case studies involving TF investigations which demonstrate that NIA and ED are able to effectively conduct financial investigations to support the investigation of terrorist activity and TF. Money trails through bank accounts and shell companies are mapped, and where necessary, assistance is sought from foreign FIUs through the EGMONT channel. India's authorities have a developed understanding of hawala trails and there are examples of the authorities following such cross-border movements of money. There are also examples of border surveillance being used to catch illicit cash movements and Goods and Services Tax information to uncover TF taking place through businesses. Authorities are able to track movements of virtual assets, an emerging TF trend in India. Although there are relatively small numbers travelling to conflict zones, intelligence agencies are cognisant of the threat from returning FTFs and they have been prosecuted in India, although mostly for non-TF offences.

351. However, the cases presented during the onsite reflected that the length of time taken from when charges are laid against the offenders and the conclusion of the trial, often takes several years. The long timelines for TF investigations, from when it is triggered to when charges are laid, have

been attributed by the authorities to the complexity of TF investigations and challenges obtaining evidence from abroad where the case has cross-border elements, as well as difficulties involved in uncovering sophisticated concealment and layering of funds. Once charges are preferred and the suspect is arrested, however, there is a statutory limit that begins from that point in time, after which the suspect is either allowed bail or remains in remand.

4

### Box 4.4. Hurriyat case

NIA registered a case in 2017 based on information that terrorist organisations, Lashkar-e-Tayyiba (LeT), Hizbul Mujahideen (HM), and Dukhtaran-e-Millat (DeM) with the support of members of the All Party Hurriyat Conference and other cross border support, were involved in terrorist activity in Jammu and Kashmir. Although 16 persons were arrested, the money trail relating to Mr Z uncovered funding from outside India from an overseas account, identified using EGMONT channels as well as information from FIU-IND. It was found that Mr Z floated several companies in India and abroad.

The overseas account opened by Mr Z received money with the assistance of his business partner, Mr Y, from other off-shore locations through hawala as well as off shore shell companies. Mr Z acted as the main financial conduit and Mr X transferred money to Mr Z to be brought into India on the pretext of a fake land purchase. The money trail from documents seized from Mr Z's chartered accountant showed that the money has been diverted to terrorists and proscribed terrorist groups as well as to Mr Y who was a leading figure in the Hurriyat Conference, having close connections with designated terrorists in the region and used funds to support their activity.

Mr Z, Mr X and Mr Y were arrested in August 2017, July 2018 and April 2019 respectively. Other suspects were also arrested. The first set of chargesheets were filed in January 2018 and supplementary chargesheets were filed in October 2019. Charges were framed against all three March 2022.

Mr Y was convicted in May 2022 on TF and other charges and sentenced to life imprisonment and a fine of INR 1million (EUR 11 111). The trial against Mr X and Mr Z is ongoing. NIA has obtained attachment orders against the assets of the offenders, including property of Mr Z which included 20 plots of land, residential premises and offices, out of which attachment orders have been issued against 17 of them INR 60 million (EUR 630 000).

### Box 4.5. Mangalore Blast case

An investigation initially registered by the State Police and subsequently taken up by the NIA arose out of a premature explosion that took place in a moving auto rikshaw in Mangalore in 2022. The explosives were meant to be planted in a temple and was funded by a network connected to ISIL. The initial investigations were focused on three suspects for their involvement in the conspiracy and procurement of the explosives.

Operational analysis received from FIU-IND revealed the use of crypto wallets to receive a large number of small amounts of funds to finance the attempted terrorist act. The investigating authority was able to obtain fund flow information from eight different VASPs to identify the accounts through which the funds were sourced from, and through IP addresses, identified the online handler who made the transfers. It was found that the suspects had used crypto-wallets of their friends and other close associates to receive funds.

Ten accused persons were arrested. Nine have been prosecuted of which chargesheets have been filed for TF under s17 and s40 of the UAPA for raising funds for terrorist acts and for terrorist organisations, against eight accused persons. They are awaiting trial.

See also box 3.2 where there is a description of the same case to highlight other aspects of it.

### Box 4.6. PFI case

A terrorist organisation had been linked to terrorist activity which included murder and public order offences and promoting ISIL ideology. The money trail was linked to 300 bank accounts in 22 branches across eleven banks across the country. In a coordinated raid in 2022, NIA searched 388 locations to seize digital devices such as laptops, mobile phones, memory cards and other digital devices, cash and other documents.

Over 150 persons were arrested and a team of 50 financial experts completed the analysis in 80 days to meet the statutory deadline for bail.

49 accused persons have been prosecuted for terrorism and TF related charges relating to sections 17, 18A, 18B and 22C of the UAPA. These involve raising funds for terrorist acts, organising terrorist camps and recruitment for terrorism. There is also a prosecution against a legal entity for TF. The PFI, a charitable organisation that was shown to spread support for terrorist activity, along with over 40 affiliated organisations, have been gazetted as unlawful associations under the UAPA. The organisation has been banned for five years and prevented from using their funds and property.

### *TF investigation integrated with –and supportive of- national strategies*

352. In the context of India, strategies relating to TF investigation are closely linked to the country's aim of countering domestic terrorism and disrupting domestic terrorist activity. MHA is responsible for the development and implementation of India's counter terrorism strategy, which is based on information gathered from agencies across the country through the MAC/SMAC mechanism. CFT features strongly in the overall CT strategy through the prevention pillar. The 2023 Action Plan that was developed to respond to findings in the 2022 NRA, includes a high-level action item for NIA and the State Police to actively pursue TF cases to disrupt terrorist networks in the

country. As noted in IO.1, more specific action items targeted in accordance with risks would be more useful to the operational agencies involved in TF.

353. In 2020 , IB (which is tasked with gathering intelligence for CT) submitted an Action Plan (2020 CFT Action Plan) which laid down a 21-point plan that reflected the multi-prong strategy to address TF within the country context. The plan covers coordination, access to data, sharing and analysis of intelligence, and a review of financing in the different theatres of terrorism as well as different modes of TF. This was collated to generate an overall shared risk understanding, identify policy priorities including the Counter-Terrorism Strategy of India, and inform red flag indicators. In addition, since 2018, the NIA, which investigates both terrorism and TF, was restructured with the number of branches across India doubling, and staffing numbers being increased significantly. The development of the NATGRID database which has been operational since 2021 has added to the resource for the central agencies investigating terrorism and TF offences to be able to access the platform directly, enabling quick access to the information needed for their investigations.

354. The national CT strategy considers the NIA and State Police as a deterrent to future terror incidents and well-defined SOPs have been adopted for terrorism and TF investigations and prosecutions. There are targets to increase parallel financial investigations by the Economic Offence Wings of State Police to be able to more actively pursue TF to disrupt terrorist networks in India. Several initiatives were undertaken to improve coordination with State Police such as collecting TF data from State authorities to identify emerging trends and patterns in TF to enhance identification, and in meetings to discuss trends and typologies themselves.

355. However, the national strategy does not adequately focus on guiding the improvement of the resourcing and expertise of the State police to be able to conduct TF investigations to support national CT strategies and investigations. For example, while there have been several capacity building programmes at the state level, no data has been provided to show that resources among the CT/CFT units within State Police have been augmented in a strategic manner to face the increasing demand of conducting financial investigations to uncover TF.

356. There is strong communication and coordination between NIA and ED, whereby an NIA nodal officer provides the node of communication between the two agencies on TF predicates through a set procedure. The procedures includes a prescribed form that contains a 'monthly statement of predicate offences' that provides an overview of predicate offences registered, details of the crime and the status of the case. ED then decides which cases to take up for ML based on its own Technical Circulars. The ML investigations by ED runs parallel to NIA's investigation of the TF offence. Although ED's Technical Circular mandates an ML investigation for all UAPA offences, only 83 ML ECIRs[95] (ML cases registered) have been filed by ED for terrorism and TF investigations over the evaluation period which is low given the TF risks in India. Aside from the broad understanding that ED investigates all complex cases relating to TF, there is no strategic guideline that dictates under what circumstances NIA would refer the ML investigation of the TF predicate, whether in accordance with the types of risks and the expertise best suited to the case, or the significance of the case and the resources required.

### *Effectiveness, proportionality and dissuasiveness of sanctions*

357. TF offences are punishable by a range of sentences under the UAPA depending on the type of support provided, all of which have high maximum sentences and some of which have minimum sentences. Raising funds for a terrorist act attracts a term of not less than five years to life imprisonment and a fine, and raising funds for a terrorist organisation attracts imprisonment of up

[95] Enforcement Case Information Report – akin to First Information Reports that are filed by the ED.

to fourteen years. Fines have ranged from INR 5 000 (EUR 55) and INR 1.075 million (EUR 11 300), which in themselves appear low. However, prison sentences, mostly between seven and ten years, provide for a dissuasive sanction, consistent with other serious crimes in India. The broad range of term of prison sentence allows for sentencing according to the gravity of the offence.

### Table 4.3. Prison sentences for TF convictions

| | 0-3 years | 4-6 years | 7-10 years | 11-14 years | 15-30 years | Life imprisonment |
|---|---|---|---|---|---|---|
| 2018 | 1 | 3 | 5 | - | - | 0 |
| 2019 | 4 | 5 | 13 | 1 | - | - |
| 2020 | 2 | 1 | 5 | - | - | 0 |
| 2021 | 02 | 0 | 7 | 2 | 2 | 2 |
| 2022 | 0 | 0 | 12 | - | - | 1 |
| Till Oct 2023 | - | 6 | 17 | - | - | - |
| Total | **7** | **15** | **59** | **3** | **2** | **3** |

358. Although the language of the UAPA appears to allow legal persons to be criminally liable for TF, no examples or data was provided of any legal persons having been convicted of TF and where a penalty was applied (see R.5, c.5.7).

### *Alternative measures used where TF conviction is not possible (e.g. disruption)*

359. Where TF charges are not possible, investigating authorities consider charges under various other laws to disrupt terrorist activity and TF such as the Arms and Explosives Act, where arms are recovered, as well as conspiracy provisions under the Indian Penal Code. This is done on a case-by-case basis.

360. Where the border trade along Jammu and Kashmir was found to be used for activity intended to move funds in support of terrorism, this trade route was closed in 2019. In regions where extortion is used to fund terrorism, State authorities have instituted measures to ensure the safety of contractors that may fall victim to extortion, as well as introducing checkpoints to search vehicles and seize cash from extortion offences. One such search at a checkpoint yielded a cash seizure of INR 12 million (EUR 133 333) that was found in a vehicle together with detonators and was to be used to fund terrorist activity planned by a Maoist related terrorist organisation.

361. The Central Government (MHA) has the ability to declare organisations as unlawful organisations by notification under the UAPA, which has been used to freeze the accounts of organisations that finance, support or take part in terrorist activity. Based on discussion with the authorities, several factors are considered in decisions to invoke this power, such as whether the organisation aims to overthrow the Indian government and/or constitution and whether the actions of the organisation are achieved through armed violence and designed to strike terror in a section of society. A lower threshold is needed for such a notification as opposed to domestic designations related to terrorism under the UAPA (see IO.10) so these powers can be used as a measure to disrupt terrorism where a TF conviction is not possible. Although any listing under the UAPA goes through a court process, there are nevertheless broad powers that are associated with this listing and thus would benefit from clearer policy articulation on the evidence and circumstances under which organisations would be considered for listing.

362. Prevention forms part of India's National AML/CFT Policy and Strategy, including counter-radicalisation initiatives. The 'sahi raasta' initiative launched in 2022, is aimed at preventing young people from being radicalised in Jammu and Kashmir where groups affiliated to ISIL and AQ operate, through national integration tours, sports programmes, skill development and festivals. Six 21-day programmes have been conducted between 2022 and October 2023, involving 161

participants. Maharashtra has also implemented a campaign to prevent terrorism allowing TF offenders to surrender so that they can be rehabilitated.

## Overall conclusions on IO.9

The NIA is well-resourced and has the expertise to enable it to identify, investigate and prosecute serious TF cases, and similarly the ED, to investigate and prosecute ML relating to TF. There are specialised CT authorities at the state level that investigate and prosecute TF, although NIA is more appropriately resourced to investigate more sophisticated cases of TF. There are several coordination mechanisms and information tools that authorities rely on effectively to identify and develop financial intelligence to support TF investigations, both between the NIA and State Authorities, and between other central authorities such as the ED. India has demonstrated that it is highly capable of investigating complex multi-faceted TF cases, including those that involve virtual assets and those with an international element.

However, while many investigations have led to prosecutions, only a small proportion of prosecutions both by NIA and the at the state level have concluded, resulting in a minimum of 1431 that remain open to date. While respecting due process, it is critical that India addresses these delays in view of accused person while waiting for the case to be tried and concluded. India's broader efforts to reduce the threat of terrorism assist with reducing potential drivers of TF.

Major improvements are needed to ensure that persons who finance terrorism are prosecuted and convicted, and subject to effective proportionate and dissuasive sanctions.

India is rated as having a moderate level of effectiveness for IO.9.

### Immediate Outcome 10 (TF preventive measures and financial sanctions)

#### *Implementation of targeted financial sanctions for TF without delay*

363. India established a legal framework in 2008 for the implementation of TFS for TF and issued revised procedures for effective and expeditious implementation in 2021 (amended twice in 2023). Under this framework, delays in communication are technically possible when new designations are made by the UN, but the Indian authorities have acted swiftly over the review period with a few exceptions. This assessment was based on a review of the Indian legal framework on TFS; statistics on designations and assets frozen; case studies showing asset freezing, attachment, and actions for non-compliance; interviews with relevant government agencies (MEA, MHA, FIU, CBI), financial and DNFBP supervisors, and discussions with FIs, DNFBPs, VASPs and NPOs.

*Designations*

364. India adopts an interagency approach to designating entities for both UNSCR 1267 and UNSCR 1373, with MHA leading the identification process. The MAC mechanism (see chapter 1) plays a central role in the designation process and coordinates with the MHA, central investigation and intelligence agencies, FIU-IND and other relevant agencies. The MAC meets regularly and discusses the merits of proposals for each target or designation developed through intelligence or investigation, where this may be placed on the agenda by any of the members. MHA then reviews the recommendations and inputs from the MAC and if it believes that the individual or organisation

fits the designation criteria under section 35 of the UAPA, the designation is notified in the official gazette of India and added to the schedule/s in the UAPA.

365. India similarly proposes listing of individuals and entities under their domestic framework through the MAC mechanism. As confirmed during the onsite via SOPs shared with the assessors, the CTCR-Division of the MHA decides whether to propose a name for domestic listing based on the individual or entity's involvement with terrorism. This includes considerations and factors such as evidence pertaining to terrorism especially for terrorist financiers operating outside of India that commit, prepare, promote or are otherwise involved in terrorism that the MAC considers before making a proposal for designation. Based on the list of designations provided to the assessment team, designated individuals were mostly founders or key members of terrorist organisations. Each gazette notification for designation contains the reasons and grounds for the domestic designation.

366. India has made four requests to propose designations pursuant to UNSCR 1373 to one country in 2022. This has not resulted in designation there and diplomatic exchanges on the issue continue. It has not received similar requests from other countries. Under this mechanism, India has listed 54 individuals and 44 organisations[96] which indicates that India is using this tool to pursue assets of terrorist financiers. Although there are processes in place, there have been no appeals or de-listing requests to domestic designations. There have been *designations* under UNSCR 1373 that have lapsed upon the death of individuals.

367. Using the same mechanism, India may propose an Indian or foreign individual or entity to the United Nations to be included in the TFS list pursuant to UNSCRs 1267/1988 and in the last five years, has made five proposals to the UNSC for designation of terrorist individuals and organisations and more recently co-sponsored three proposals during its rotating membership to the UN Security Council

### *Communication and implementation of new designations*

368. Implementation of TFS for TF in India begins when the MEA sends a communication electronically to nodal officers at each regulatory authority when there is a designation or change in designation made by the UN, which must be done 'without delay.' In parallel, changes to the UN list are also posted to the FIU website as well as electronic communication via the FINGATE portal to registered reporting entities. An Official Memorandum was issued in October 2023 clarifying that without delay in the context of TFS for TF (and PF) means "within the same business day not later than 24 hours." The authorities' intent with this clarification was to alert all natural and legal persons to also check the FIU website for TFS changes and to explain that "sanctions are imposed 'without delay' as required in different International Conventions." Notwithstanding the intent of the October 2023 OM, a plain reading of the regulations with this definition creates a potential legal loophole of two 24-hour periods when the MEA sends a communication to reporting entities followed by reporting entities taking another 24-hours to implement.

369. In practice, based on a review of electronic communication and interviews with the MEA, FIU, regulators, and reporting entities, this communication has been issued well within 24 hours by the MEA to nodal officers to reporting entities in most cases between January 2020 and late-2023.[97] There are outliers which India has explained to be due mainly to technological reasons and other reasons unrelated to the process (see table 4.3). To prevent future delays due to technological reasons, regulators revised their Circulars to clarify that their reporting entities should check the

[96] The listing can be found on the MHA website – Terrorist organisations under Schedule I and individual terrorists under Schedule IV of the UAPA.

[97] Data prior to that is not retrievable due to a technical issue caused by email migration.

UN website directly, the FIU and MEA websites, in addition to receiving the communication from designated UAPA nodal officers.

### Table 4.4. Release of MEA's Order (January 2020 to June 2023)

| Year | Released within 24 hours | Released between 24 and 30 hours | Reasons for delay | Released more than 30 hours | Reasons for delay |
|---|---|---|---|---|---|
| 2023 | 5 | 1 (30 hours) | Unable to access UN press release | 1 (49 hours) | Global email outage of MEA |
| 2022 | 7 | 1 (29 ½ hours) | Officers busy in Republic Day duties | 1 (35 hours) | NIC mail server downtime (MEA to nodal officers) |
| 2021 | 7 | 0 | 0 | 1 (35 ½ hours) | Medical emergency of the officer in charge (MEA) |
| 2020 | 10 | 0 | 0 | 0 | |

370. During interviews with various designated nodal officers, they indicated that they send forward the designated list immediately upon receipt of a notification from the MEA to the regulated entities so the whole process (MEA to Nodal Officers to reporting entities) occurs within 24 hours. Nonetheless, to minimise delay in communicating updates to the lists, the FIU also sends alerts communicating the changes through the FINGATE portal to registered reporting entities s. However, not all reporting entities are registered on the portal (see Chapter 1). Both the MEA and the FIU have links to the UN consolidated list which reporting entities are required to check regularly.

371. The OM sets out in detail the process required for different regulated entities should a match be found. Regulated entities are required to take action as prescribed for each type of entity by the OM For example, financial institutions and DNFBPs shall prevent designated persons from conducting financial and related transactions. Where there are assets, financial institutions and DNFBPs are required to inform the relevant authority with 'full particulars' of the designated entity's assets so that freezing orders may be issued.

372. Financial institutions and VASPs are also required by their regulating authority to maintain updated lists of designated individuals and entities, checking once a day whether their customers hold assets on or behalf of those designated. If they detect a match, they must immediately inform the relevant nodal officers and the FIU, submitting an STR, and prevent the designated person or entity from conducting any transaction. Discussions with most types of reporting entities, in particular FIs, indicated that they understand that they should check the UNSCR and/or the MEA list or FIU website daily and those with commercial sanctions screening products also rely on them. Some DNFBPs are still acquiring commercial software or building monitoring systems with these requirements and thus are relying on a communication from their nodal officer.

373. India provided a case example where a VASP found a match of an associate of a UN designated terrorist in its customer database. The name of the alleged associate was triggered based on media reports when he was arrested by NIA for narcotics smuggling. Based on the name and photographs, the VASP identified a positive match with the alleged associate, blocked the virtual assets account worth INR 27.5 million (EUR 310 000) on 14 June 2023 and filed an STR with the FIU. The VASP then informed MHA on 26 June 2023. MHA carried out an inquiry and on 8 November 2023, and informed the VASP that no terror link could be established between the alleged associate and the UN designated terrorist. The account was released.

374. For all other natural and legal persons, the obligation under the August 2023 corrigendum to the OM, the obligation is phrased in a way that requires them to inform the nearest police station, which would then inform the state nodal officer who would then start to process to issue the

freezing order. While the understanding of the Indian authorities is that the corrigendum in effect creates a freezing obligation, streamlining the language so that obligations and the steps entities are expected to take is reflected clearly and consistently in the OM and the respective guidance documents would facilitate entities' understanding, especially DNFBPs and other natural and legal persons.

375. Financial regulators have been conducting outreach and training for their respective reporting entities consistently over the assessment period. As the regulator of VASPs, FIU-IND has conducted extensive engagement with VASPs and also conducted review exercises on their compliance with AML/CFT obligations, including TFS obligations. There have also been some outreach and training exercises delivered to DNFBPs as part of a broader AML/CFT outreach, although these have been more recent and limited (see IO.1 for a more in-depth description of the AML/CFT outreach to reporting entities).

376. While established FIs and VASPs were aware of their obligations and had the necessary structures (such as sanction screening software) and knowledge to meet their obligations, this was not the case for DNFBPs, especially those that have been designated as reporting entities under the PMLA more recently. Some DNFBPs that the assessors met during the onsite had only recently started conducting screening against the relevant sanctions lists by using a manual process before onboarding a new customer, and were not clear as to the next steps required, particularly in relation to dealing with the assets and the designated entities themselves if they were to identify funds or other assets associated with a designated person or entity (see IO.4). This is consistent with the fact that the OM (before the August 2023 corrigendum that clarified the obligation for DNFBPs) as well as the associated guidance issued, is silent on the obligation placed upon DNFBPs to immediately freeze assets held or not to continue dealing with the designated individual or entity, as there was an additional process required to inform their respective nodal officer, who will then facilitate a process though MHA to obtain a freezing order before the entity is required to implement the freeze.

377. The process for domestic designations under UNSCR 1373 is similar to designations made and electronically communicated by MHA directly to nodal officers. Once approved, the list is updated on the MHA websites and alerts are sent electronically to nodal officers in regulatory agencies such as MCA and CBIC, to the financial sector regulators as well as to FIU-IND. The nodal officers then immediately forward the list to regulated entities at which point they are required to update their own lists of designated persons. FIU-IND uploads the list on FINGATE and registered reporting entities are sent regular notifications through the system. The authorities informed the assessment team that in practice, communication is done without delay.

378. Two accounts were frozen in India pursuant to UNSCR 1267 involving a total sum of INR 2.684 million (EUR 32 000). Twenty-eight properties (asset value not provided) had been attached of persons who have been domestically designated under UAPA during the evaluation period.

4

### Box 4.7. Freeze by Bank of designated persons (UNSCR 1373)

Based on a notification of a domestically designated persons under UNSCR 1373 dated 6 and 7 January 2023 under the UAPA list, the J&K Bank reported on the 7 January 2023 that there was a match against two of its customers. The Bank immediately froze the accounts and filed STRs with FIU-IND. The matter was also referred to central security agencies on the same date.

On 13th April 2023, IB confirmed the match and the accounts were frozen under the UAPA on 11th August and 29th September, which remains frozen while the NIA is investigating the individuals.

379. Before the August 2023 corrigendum to the OM was issued, there was no clear legal obligation for natural and legal persons other than reporting entities to implement targeted financial sanctions pursuant to UNSCR 1267 and 1373 without delay (within 24 hours), with the exception of a number of public bodies listed in the original memorandum such as land registry. The correction broadened the obligation by requiring that any person, either directly or indirectly, holding funds or other assets of designated entities to freeze any transaction in relation to such funds and inform the relevant authorities. However, as noted above, the language in the corrigendum does not categorically require natural and legal persons to freeze assets, but to follow a process which will lead to a freezing order being issued.

## *Targeted approach, outreach and oversight of at-risk non-profit organisations*

### *Identification of NPOs at risk of TF abuse*

380. While TF vulnerabilities and the sources and channels for TF remain dynamic in India, the NRA takes into account mitigating measures instituted by the country and has assessed the national TF risk as medium (see IO.1). Within this context, India conducted a sectoral risk assessment of NPOs (NPO SRA) in March 2023 which considered the use of NPOs for TF within the six different theatres of terrorism identified in the NRA, with a residual risk rating incorporated into India's overall assessment of TF risk. The NPO SRA identified that religious-based NPOs that are vulnerable to radicalisation activities and NPOs located in two specific regions, faced higher TF risks than other regions, although the overall risk was low.

381. ITD has undertaken an exercise to identify the universe of NPOs operating in the country. NPOs that are registered under section 12AB of the ITA as charitable organisations enjoy tax exemptions, through which tax authorities collect verification documents and put in place ITA-specific compliance requirements. Every NPO filing a tax return, whether or not registered for a tax exemption, is given a unique Permanent Account Number (PAN). Eligible NPOs that do not register under section 12AB would attract the attention of the authorities to understand why they would prefer to incur higher tax liabilities. Even NPOs receiving contributions below the threshold will need a PAN number to open a bank account. Therefore, although they would invariably be low risk for TF abuse on the basis of the minimal amounts of funds they receive, they would remain within the visibility of the authorities. Through its tax evasion detection mechanisms, ITD is also able to identify NPOs that have significant financial transactions but have not filed income tax returns.

382. Given the above, in effect, all legitimate NPOs operating in India that receive contributions above the tax threshold would be registered with the tax department. As of March 2023, 286 260 NPOs were registered under section 12AB of the Income Tax Act. Based on the theatres of terrorism, the identification of religious NPOs in five states and all NPOs in another two states, as of March

2023, a total of 6 648 NPOs have been identified to be "at-risk" in the country. This increased to 7 500 in October 2023 on account of more NPOs registered between the period.

383. The basis for identifying the 7 500 NPOs at risk is the calculation of a combination of data points relating to the geographical location of NPOs, their function (e.g., religious), channels of funding, intelligence information relating to their activities that India has used to assess that they pose higher risks of abuse or misuse as well as information obtained based on responses from questionnaires from NPOs. These questionnaires considered aspects of general integrity requirements, understanding of the background and affiliations of board members, employees, fundraisers and volunteers, internal financial and personnel controls.



*Registration requirements*

384. NPOs are required to be registered with multiple government authorities and comply with the different regulations depending on their structure as well as size and source of funds. For example, NPOs that receive contributions beyond INR 250 000 (EUR 2 778) must be registered under the Income Tax Act (ITA). NPOs are required to provide documents on registration (renewable every five years) that indicate their charitable objects and activities. PML Rules require that reporting entities maintain a record of transactions with NPOs over INR 1 million (EUR 11 111). A Statement of Financial Transactions of the NPO be filed by reporting entities with CBDT as well as their expenditure through a Tax Deduction at Source (TDS) mechanism which are also available to ITD. NPOs that are legal persons are also registered under the Companies' Act and those that are societies or trusts must be registered according to their respective State's Societies Registration Act. NPOs that receive foreign contributions are further required to register under the Foreign Contribution (Regulation) Act (FCRA).[98] NPOs can register under the Darpan portal to be eligible to receive these funds, as well as other grants offered by the government. The Darpan portal currently has over 185 000 NPOs registered and serves as an online repository of information on these NPOs.

385. Each piece of legislation has its own set of registration information required to be filed as well as its own set of compliance requirements, the violation of which can result in penalties being imposed on the NPOs or its activity suspended altogether.

*Monitoring and outreach*

386. The principal authority that has the responsibility to undertake monitoring and outreach for the prevention of NPOs being abused for TF, in conjunction with its monitoring for irregularities in tax reporting, is the ITD. The ITD uses two risk-profiling aids to identify entities, which may include NPOs, for verification of their tax documentation. These risk-profiling aids, the Computer Aided Scrutiny Selection (CASS) and the Risk Management Strategy (RMS), select cases for scrutiny based on data provided under the ITA, information shared amongst government authorities such as MAC, FIU-IND and intelligence collected by authorities such as the IB. The main difference between the two systems is the breadth of case selection under each system. The CASS selection covers entities that have filed tax returns in the last tax year, while the RMS selection also covers entities that have not filed taxes and is not limited to the last tax year. While the focus of these mechanisms is primarily to ensure tax liabilities and exemptions are being appropriately applied, they have been used to identify NPOs that were being used as a vehicle for TF or were at risk from being so due to irregularities identified in their documentation. Between 2018 and 2023, 31 405 NPOs were identified for audit under the CASS and RMS, out of which 7 735 violations for taxes under the ITA were found. In 87 cases, for more serious violations, the s12AB registration of NPOs

[98] Companies operating in India are required to spend a minimum of 2% of their net profit on corporate social responsibility (CSR) activities. See Chapter 1.

were cancelled and out of these, three irregularities related to TF and were referred to the relevant LEA for investigation. Investigations found that these NPOs were collecting donations from abroad meant for charitable means and diverting them for activities to incite terrorism in an identified high-risk region.

387. Where an NPO is registered as a society, the respective state Charity Commissioner is also empowered under their respective State's Societies Registration Act (the Registration Act) to obtain information on the charitable entity through the Memorandum of Association, membership and office-holder information. State authorities are the first regulatory interface when an NPO is formed, and their regulatory requirements add the first layer of financial prudence requirements. Charity Commissioners are able to sanction or dissolve non-functioning NPOs registered as societies, as well as those that have contravened requirements of the Registration Act. However, monitoring is done wholly at the State level and in accordance with State laws and requirements which are not consistent across India. Further, their focus is on general organisational integrity and financial transparency, and they have limited expertise with monitoring entities specifically to prevent TF abuse. For example, the Charity Commissioners do not generally have access to intelligence from MCA, FIU-IND as well as intelligence collected by authorities such as IB in the way that the ITD does.

388. In India, all NPOs that receive funds from foreign countries must be registered under the FCRA which is a national security legislation that first enacted in 1976 to regulate the inflow of contributions and aid into the country. The intention behind the Registration Act was to regulate the acceptance of foreign contribution or hospitality by certain individuals or organisations and to prohibit acceptance and utilisation of this for activities detrimental to national interest. Aside from NPOs (which is defined in the FCRA as any person "having a definite cultural, economic, educational, religious or social programme"), the legislation also covers political parties, government employees, judges and media outlets. Since then, the legislation has been through several amendments that have resulted in stronger regulations that apply to entities covered under the framework.

389. Under the FCRA, all NPOs that seek to receive foreign contributions must obtain a certificate and strict criteria are prescribed to obtain one. Aside from general integrity rules, the NPO is required to work for three years and spend a minimum of INR 1.5 million (EUR 16 667) on welfare activities for the benefit of society before it may apply for FCRA certification. Foreign funds can only be received to a specified bank account and contributions must be reported to the MHA. These funds must be used directly towards the charitable cause and cannot be outsourced to another local entity that may be engaged by the NPO. A certificate once obtained, may be cancelled or suspended for violations under the FCRA. India reported that in the last five years, 1 828 registrations have been suspended or cancelled and 1 260 registrations have not been renewed. Of these, the registration of 21 NPOs were cancelled or not renewed due to their involvement with terror or radical activities or supporting terror or radical activities.

390. As the scope and purpose of the FCRA is broader than and not primarily intended to prevent TF, NPOs receiving foreign contributions under this legislation have not specifically been assessed as for the subset of "at-risk" NPOs in the risk assessment on NPOs on TF abuse. Requirements under the FCRA are imposed equally on all NPOs receiving foreign funding. India has nevertheless identified the FCRA to be useful in mitigating the threat relating to TF abuse of NPOs through the receipt of foreign funds due to the enhanced oversight and control of the inflow of funds to the country, noting that this is not a risk-based process.

391. The assessment team met with six NPOs during the on-site visit, of different sizes, representing different levels of risk, located in different regions and involved in different types of good works. All the NPOs communicated the view that the compliance rules put in place by the

authorities were important to prevent abuse of NPOs. However, the NPOs demonstrated superficial levels of understanding of TF risks relating to their geography or type of activity. While they were aware of the importance of ensuring that their funds came from legitimate sources and the importance of using banking platforms to collect contributions from both domestic and foreign sources, the NPOs were not aware of the findings of the risk assessments related to TF, including the common channels used for TF in 'their theatre'. NPOs were aware that they should use contributions in accordance with the purpose of the charity. However, other than this, there was little focus on ensuring that the end-use of the funds did not inadvertently involve support for terrorist activity, terrorists or terrorist organisations, as the NPOs were not adequately sensitised to the wider risk of TF abused through NPOs.

392. All NPOs reported ongoing engagement with different authorities (mostly ITD and IB), the focus of which was on ensuring compliance with their respective legislative requirements. It did not appear that the authorities coordinated with each other in conducting outreach and each was focused on compliance with their own framework and sphere of concern. Based on discussion with NPOs, the assessment team was concerned that NPOs are burdened with laws and procedures with the stated intention of mitigating TF abuse of NPOs, among other purposes, but the authorities do not focus outreach on the NPOs that are vulnerable. In addition, NPOs have not been subject to consultation to develop and refine best practices to address TF risks and vulnerabilities so that they are protected from TF abuse, nor on input to develop risk assessments and TF policies and legislation that would also affect NPOs and their work. For example, although TF was not central to the 2020 amendments under the FCRA, these were implemented without adequate consultation with NPOs, impacting their activity or operating models. This resulted in NPOs not being able to use foreign funds through third party implementers and negatively impacted the operating models of some NPOs.

393. NPOs indicated that they are reliant on privately created eco-systems through their own networks to navigate the changes in the different laws and registration processes in the absence of clear and timely guidance from the state or central authorities. This impacts the ability of NPOs to focus their efforts undertaking the 'good works' without necessarily any effective vigilance on their part to address the possibility of TF abuse.

394. As corroborated by the NPOs, IB has conducted engagement with some higher risk NPOs to familiarise them with IB's process and recently introduced checks on sources of funds, and to better understand their vulnerabilities to TF abuse. Information collected through these engagements was fed into the NPO SRA. Since 2018, ITD has been conducting about 40 outreach programmes annually. However, no information was provided on the frequency of these programmes for at-risk NPOs or what was communicated to them. In view of this, the assessment team was not able to conclude that the outreach programmes to NPOs were adequate and risk based. In particular, it was not clear to what extent outreach was prioritised or targeted at the subset of 7 500 NPOs identified to be "at risk" of TF abuse. There was no indication of the ITD working with the other authorities conducting outreach programmes to come up with strategies or SOPs to ensure that outreach was conducted in a consistent, targeted and risk-based manner. This did not give the assessment team the confidence that outreach undertaken by ITD was properly targeted to prevent TF abuse rather than just irregularities of its financing regulations under its framework.

395. Further, aside from minimal engagement by the Charity Commission with the current donors of some NPOs, insufficient information was provided on the existence or extent of any broad educational or awareness raising programmes to target potential donor communities to sensitise them about their role in minimising potential vulnerabilities of NPOs to TF abuse and TF risks.

### *Deprivation of measures TF assets and instrumentalities*

396. Deprivation of assets belonging to terrorists and terrorist organisations and related to terrorist activity, is achieved in India through multiple mechanisms with varying results. India has applied TFS in line with UNSCR 1267 and proposed the listing of five terrorists. Two accounts including one related to a VASP, have been frozen in India pursuant to UNSCR 1267 involving a total sum of INR 2.684 million (EUR 32 000). India has also designated 44 terrorist organisations and 54 individuals under UNSCR 1373. Between October 2020 and June 2023, a total of INR 27.5 million (EUR 305 555) has been seized by MHA from 76 bank accounts and 28 properties pursuant to UNSCR 1373.

#### Box 4.8. Freezing following designation under UNSCR 1373

In 2022, India designated under the fourth schedule to the UAPA, the commander of a terrorist organisation (HM) who was instrumental in co-ordinating terrorist activities in Jammu & Kashmir, and was involved in TF and smuggling of arms, ammunition and explosives in the region. He was also involved in coordinated killings and terror attacks in the region as well as recruitment of terrorists. The said commander left the country and in March 2023 and investigations by NIA revealed his property in northern Kashmir valued at INR 2.5 million (EUR 28 000). Consistent with their powers under UAPA, NIA issued an attachment order on the property.

397. Where a person or entity is being investigated for TF offences under the UAPA, India also has broad powers to seize TF assets and instrumentalities even without the need for a UNSCR 1373 designation. The UAPA was amended in 2019 to empower the Director-General of the NIA to grant approval to seize property acquired from proceeds of terrorism anywhere in India, without having to seek permission from the State Police. Since then, the NIA has increasingly used this power to pursue assets relating to terrorism and TF (see table 4.3). These include both moveable and immoveable property, (the large jump in amounts frozen in the first half of 2023 is attributable to one case relating to left-wing extremism which resulted in the seizure of property as well as over 150 accounts.) The Indian authorities have confirmed that in all cases, the seizures relate to TF cases where the definition of terrorist act and consequently TF is within the parameters of R.5 (See IO.9). NIA has not pursued the seizure of property relating to TF outside India. Based on the cases presented, there is a strong cross-border element to TF in India, and it would benefit NIA build its expertise and networks to be able to pursue TF assets abroad where appropriate.

#### Table 4.5. Assets seized/attached under the UAPA by NIA (excluding freezing under UNSCR 1373 obligation)

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (until Oct 23) |
|---|---|---|---|---|---|---|
| Nos of persons | 4 | 6 | 11 | 20 | 8 | 31 |
| Nos of cases | 4 | 2 | 7 | 10 | 5 | 20 |
| Value of assets | EUR 361 785 | EUR 280 thousand | EUR 350 thousand | EUR 1.5 million | EUR 1.14 million | EUR 6 million |

398. State Police who investigate TF are also empowered to identify and seize the property of terrorists. This has been done in 116 cases since 2018 (see Table 4.6) from bank accounts and other assets. However, the pursuit of terrorist assets at the State Police level takes place less strategically and with a view to collect evidence rather than disrupt terrorist activity, although consistent with their primary responsibility to prevent, detect and deal with terrorism and funding of terrorism at the State level.

**Table 4.6 Assets seized by the State Police in India for TF investigations**

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (until Oct 23) |
|---|---|---|---|---|---|---|
| Value of assets | EUR 4 000 | - | - | EUR 112 000 | EUR 1.5 million | EUR 235 317 |

399. The Enforcement Directorate (ED) also conducts ML investigations where TF is the predicate offence, and the ED is able to access broad powers to trace and seize assets under the PMLA (see IO.8). Between 2018 and 2023, ED has conducted 48 investigations where it has seized INR 10.62 billion (EUR 118 million) ML proceeds related to TF. Of this INR 8.59 billion (EUR 95.5 million) has been seized within India and INR 2.03 billion (EUR 22.5 million) has been seized abroad.

400. The figures illustrated that the Indian authorities, especially NIA, have consistently pursued assets of terrorists, terrorist organisations and terrorist financiers, as part of their pursuit of TF. There is no data to show how much has resulted in confiscations.

### *Consistency of measures with overall TF risk profile*

401. India has two designation tools that it uses to pursue assets of terrorists, terrorist organisations and terrorist financiers. The first is the UNSCR 1373 designation tool undertaken through an inter-Ministry mechanism coordinated by MHA through which it had designated 44 terrorist organisations and 54 individuals as at the end of the onsite. At the same time, India has the ability to proscribe terrorists and pursue their assets under the UAPA, which is undertaken by NIA during its investigations, in consultation with other related authorities. India utilises these tools in line with its TF risks. However, there is no overarching strategy as to when one mechanism is used instead of the other despite both proscriptions are based on the entities' involvement with terrorism.

402. The 2019 amendments to the UAPA broadening NIA's powers to seize assets of terrorists and terrorist organisation, reflects India's developing understanding of how powers to seize assets riding on designations or TF investigations is useful to prevent terrorists from raising, moving or using funds. Case studies provided by the authorities reflect how the NIA has used these powers to deprive terrorists of funding in the different theatres of terrorism identified in the NRA. The establishment and access to the NATGRID database (see IO.9) supports the central agencies with their pursuit of assets relating to terrorism.

403. As disruption is the priority, central agencies focus on asset seizures rather than confiscations as confiscation requires the conviction for the terrorism or TF offence. While the case is pending, the authorities consider the ability to disengage the suspected terrorist from his funds that may go towards another terrorist attack, is a valuable tool. This is less evident for State Police investigating TF.

404. India's strong emphasis on disruption and prevention mechanisms for terrorism and TF is in line with TF risks overall. However, some measures, particularly relating to preventing the NPO sector from being abused for TF, are not calibrated to the nature of the risks.

## Overall conclusions on IO.10

India has an interagency framework to designate entities for UNSCRs and uses this tool to designate terrorists and terrorist organisations as part of its CT strategy. However, while it has a legislative framework to communicate updates to the UNSCR lists, due to the complexity of the framework, reporting entities, in particular DNFBPs and less established FIs, are not

clear on their obligations in on what they need to do when they find a match. Two accounts have been frozen and twenty-eight properties have been attached based on TFS matches during the evaluation period.

India has several parallel legislative mechanisms that it uses to address the risk of NPOs being used for TF abuse. However, implementation, as well as NPO outreach conducted by authorities under these mechanisms, are not coordinated or risk based.

India pursues assets of terrorist and terrorist entities and has seized a significant amount of funds and assets, which reflects the agencies' understanding of how powers to seize assets riding on designations or TF investigations is useful to prevent terrorists from raising, moving or using funds.

There is a lack of coordinated strategy on the use of the different designation tools for the pursuit of TF in the country. India's strong emphasis on disruption and prevention mechanisms for terrorism and TF is in line with TF risks overall. However, some measures, particularly relating to preventing the NPO sector from being abused for TF, are not calibrated to the nature of the risks.

India is rated as having a moderate level of effectiveness for IO.10.

## Immediate Outcome 11 (PF financial sanctions)

405. India is committed to counter-proliferation as demonstrated by its framework established to prevent proliferation of sensitive goods and technology in accordance with its national and international commitments. India implements UN sanctions through the United Nations Security Council Act of 1947 in line with its obligations to implement UN sanctions as a UN member. In addition, India has its own autonomous sanctions regime. Although India is a producer of dual-use goods, it maintains control on the trade of these goods through its strict licensing regime (see core issue 11.2).

406. India has no common borders with DPRK. It has diplomatic relations with DPRK and its exposure to DPRK is mainly related to trade, which is predominantly in medical and agricultural products. However, trade is heavily restricted, has significantly declined since 2019, and is currently at an insignificant level (see Chapter 1). Further, trade with DPRK is only permitted through one State bank which must conduct EDD on transactions.

407. India is not a major transit hub for international trade as most of the Indian cargo traffic is destined to or originated from India. There is some possible exposure from trade and transhipment through cargo traffic and as India emerges as a financial centre (see Chapter 1).

### *Implementation of targeted financial sanctions related to proliferation financing without delay*

408. Similar to TFS for TF, India maintains a multi-agency approach to all PF sanctions emanating from the UNSCRs. The law and the regulation under it, established on 30 January 2023[99] disallows the financing by any person of any activity which is prohibited by any UNSCR in relation to weapons

[99] Based on Order 12011/14/2022-ES Cell-DOR dated 30th January 2023 (WMD Order) issued under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005 (WMD Act).

of mass destruction and their delivery systems.[100] Under the WMD Order, the MEA is responsible for communicating "without delay," changes made to Director of FIU-IND as the Central Nodal Officer as well as other Nodal Officers including regulators, who communicate the updates to reporting entities. At the same time, updates are also communicated to registered reporting entities when the FIU uploads the updates to FINGATE and publicly on the FIU website. The WMD Order has a clearly phrased umbrella provision that mandates all natural and legal persons holding funds or other assets of designated persons and entities, to freeze the funds and assets, without delay and without prior notice, so that the legal obligation starts as soon as the person or entity is designated by the UN and communicated by the MEA. Further, on 30 October 2023, India issued an update to the regulation to clarify that the meaning of 'without delay' as "preferably on the same business day but not later than 24 hours in any case."



409. Communications data provided since January 2020[101] indicates that six designation communications from the time of the UNSCR consolidated list posting and the MEA communication to regulators took place within 24 hours and one communication for SC/15342 took 73 hours caused by the inability to access the UNSC press release. MEA's internal SOP based on WMD Order requires that the UN website be monitored at least twice on a daily basis and to stay in regular contact with the Permanent Mission of India to the UN and/or his/her back-up officer.

410. The current communication mechanism of India's CPF obligations through FIU-IND and nodal officers as per the WMD Order as well as a clearly articulated legal obligation to freeze without delay, has only been recently established. Prior to 30 January 2023, the general prohibition of financing of sanctioned entities by the UNSC was based on the United Nations (Security Council) Act of 1947 and provisions of the WMD Act, in particular s12A of the WMD Act as well as MEA Orders related to specific UNSCRs. Under this regime, MEA sent electronic communications to RBI, SEBI and IRDAI who also sent the MEA communications to their regulated entities without delay. Besides this, entities using sanctions screening software were engaged in screening for PF related sanctions for DPRK and Iran. Although the UNSC sanction lists would be published on the website of MEA, the FIU-IND red flag indicators for STR filing also required the reporting entities to screen customers and transactions for matches with UNSC sanction lists.

411. Prior to January 2023, some FI regulators published lists of designated individuals and entities relating to PF. For example, SEBI conveyed sanctions lists through their websites and sent it to entities registered under it. RBI also circulated UNSCRs from time to time for reporting entities regulated by it. While there was some engagement on sanction screenings for reporting entities regulated by RBI, SEBI and IRDAI, this was not the case for all reporting entities, especially DNFBPs, and it was not clear whether there was an explicit requirement directed at all reporting entities for this to be done without delay. The change was instituted in January 2023 to formalise and streamline the communication to regulators through the FIU-IND, particularly with the use of FINGATE and the FIU website to communicate updates to reporting entities as well as all natural and legal persons.

[100] This would include UNSCR 1718 & its successor resolutions (DPRK), and UNSCR 2231 (Iran) prior to the expiration on 18th October 2023. As no funds and assets were identified or frozen in respect of UNSCR 2231 in India, no de-listing or unfreezing requests have been made or are expected.

[101] Similar to TFS (IO.10), data prior to that is not retrievable due to a technical issue caused by email migration.

### *Identification of assets and funds held by designated persons/entities and prohibitions*

412. At the time of the onsite, no property had been frozen pursuant to counter-proliferation TFS in India. To date, there have been no matches with designated lists under UNSCR 1718 and its successor resolutions reported to MEA or FIU-IND through sanction screening under the WMD Order (post-January 2023) or generally under the WMD Act (pre-January 2023), nor the one-time screening process (see below). Accordingly, there have been no requests for de-listings or unfreezing requests.

413. As part of the onboarding process of the current implementation mechanism, FIU-IND undertook a one-time sanction screening exercise with reporting entities by sending an alert to them through FINGATE in January 2023. The intent of this exercise was for FIU-IND to make contact with all reporting entities as the new central nodal officer for PF TFS, to make sure communications were working and to establish if any implementation gaps existed. This resulted in over 170 000 false positives received from twelve financial institutions, but no funds or other assets of designated entities were identified. FIs were not required to file a report stating that they found no true matches and the exercise itself cannot guarantee that no matches existed before the FIU took over as the central nodal officer. However, given India's exposure to PF is low the results are somewhat expected.

414. The fact that no PF funds and assets have been identified in India is consistent with India's relationship with the DPRK as transactions are limited to just one specific financial institution that applies EDD for the processing of humanitarian transactions (medical supplies and agricultural goods), and the fact that authorities are active in the implementation of broader counter-proliferation measures through a robust licensing requirement for dual-use goods, as well as goods that are identified as strategic in nature or destined to sanctioned countries (or other destinations or end-users that the authorities may have concerns with). The Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) licensing regime involves a multi-agency mechanism for the licensing of exports of dual-use goods and technology which considers document verification as well as assessment and verification of end use and consideration of financial intelligence. Examples were provided where, on the basis of information obtained through the SCOMET mechanism, further investigations into individuals and entities from sanctioned countries were conducted for licences to import or export goods.

415. Interviews during the onsite at Maharashtra's Jawaharlal Nehru Port showed that Customs had sophisticated understanding of import, export as well as transhipment risks relating to sanctioned countries and is alive to typologies being used to evade targeted financial sanctions though misdeclarations of goods or entities involved. Customs also receives MEA communication on PF sanctions which is fed into its computerised risk management system to identify potential funds/assets movements of sanctioned entities. Where there is suspicion, customs authorities are also able to conduct BO checks on entities.

416. The lack of assets seized in India is consistent with the strict licensing measures put in place, strong sanctions evasion detection as well as the low exposure to DPRK through trade and diplomatic activity.

### *FIs, DNFBPs and VASPs' understanding of and compliance with obligations*

417. Similar to TFS for TF, the assessment team found that while established FIs and VASPs were aware of their obligations and had the necessary structures (such as sanction screening software) and knowledge (including on sanctions evasion techniques) to meet their obligations, this was not the case for some DNFBPs (see IO.10). Larger and more established reporting entities, especially

FIs, have been using commercial software designed to fulfil their legal obligations globally, to run sanction screening independent of the lists shared by MEA or on FINGATE, even prior to 30 January 2023. The variation in their understanding of, and approach to implementing TFS on the part of DNFBPs can be attributed to the fact that the incorporation of several DNFBPs as reporting entities as well as the issuance of the WMD Order by DOR and related guidance by the regulators took place only recently.

418. While a large number of false positives were detected during the process of the one-time sanction screening of reporting entities, no matches have been received by the FIU on PF TFS to date as the WMD Order requires this only when there is a match.

### *Competent authorities ensuring and monitoring compliance*

419. Regulators of FIs, DNFBPs and VASPs have included PFs sanction screening obligations in their respective guidance and circulars, which have been issued by the various regulators between March and September 2023. FIU-IND has also prepared a detailed Best Practices Guide for Implementation of TFS Related to PF based on the regulatory requirements as well as information collected from outreach to FIs and VASPs, which was released on FINGATE in July 2023. Based on the Guide, there appears to be a push by FIU-IND to encourage reporting entities that have not already done so, to use commercially available automated systems to conduct sanctions screening. While this is useful for larger FIs, smaller REs including DNFBPs will invariably not have the resources to rely on commercial sanction screening tools and would thus require more guidance targeted towards their circumstances, including ideally awareness of sanctions evasion techniques relevant to their sector.

420. In 2023, a significant number of outreach exercises were undertaken by FIU-IND to FIs, VASPs and several DNFBPs on PF TFS and sanction screening obligations. Outreach exercises to DNFBPs in precious metals and stones real estate and TCSP sectors have been undertaken by their respective professional bodies as part of AML/CFT/CPF obligations as reporting entities. However, specific outreach on PF TFS obligations conducted to FIs have been significantly more than to some DNFBPs such as real estate agents.

421. All on-site inspections of FIs and VASPs conducted by RBI, SEBI and FIU-IND cover PF TFS obligations. The focus of these inspections has been to identify and assist with challenges faced by the entities in complying with their obligations related to sanctions. In the last five years, based on its supervision, RBI encountered twelve instances of compliance shortcomings on TFS while SEBI has not come across any instance of non-compliance with screening obligations. The observations made were incorporated into the inspection report for the bank and followed up upon until compliance was achieved. Supervision on two VASPs were conducted in July 2023 by FIU-IND. No concerns were raised with regards to sanctions screening for one VASP while time sensitivity of sanctions screening was communicated to the other VASP during its onsite assessment. No statistics were provided in relation to the other regulators during the evaluation period, including CBIC that regulates real estate agents (REAs) and dealers of precious metals and stones (DPMS). In November 2024, CBIC issued guidelines for supervision of reporting entities on a risk sensitive basis that will apply to REAs and DPMS for PF.

422. Since January 2023, FIU-IND has been involved in developing the expertise of compliance monitoring in India with a view to providing clarifications and developing reporting entities' understanding of sanctions screening in a phased manner. FIU-IND has reviewed questionnaires to reporting entities on the implementation of TFS which was assessed against the Guide on Best Practices for Implementation of Targeted Financial Sanctions Related to Proliferation Financing, developed by FIU-IND. In 2019, FIU-IND imposed a penalty of INR 1.04 million (EUR 11 500) on a public sector bank for several compliance failures, including the failure to fully implement a CDD

programme with regards to screening names of prospective customers in the latest UNSC sanction list.

423. Some DNFBPs are at a nascent stage of understanding and implementing TFS obligations and will benefit from outreach by the FIU-IND to help them develop their expertise.

## Overall conclusion on IO.11

Since January 2023, India's PF TFS implementation mechanism has been laid out in the WMD Order and designations are linked to the MEA website, and electronically communicated by MEA to relevant agencies and on FINGATE by FIU-IND without delay. MEA also communicates PF TFS updates to regulators under the WMD Order. Although the obligation not to finance sanctioned entities existed before January 2023 under the WMD Act and the United Nations (Security Council) Act supplemented by MEA Orders, it has not been demonstrated that this was being implemented by all reporting entities and that it was being implemented without delay.

To date, there have been no matches with designated lists under UNSCR 1718 and successor resolutions (DPRK) reported to MEA or FIU-IND through sanction screening under the WMD Order. or generally under the WMD Act, nor as a result of the one-time screening process. This appears to be consistent with the limited exposure of India to PF activity as well as strict licensing regime and emphasis on sanctions evasion detection techniques.

However, while established FIs and VASPs were aware of their obligations and had the necessary structures (such as sanction screening software) and knowledge to meet their obligations, some DNFBPs that have been more recently been incorporated as reporting entities, do not have the same level of awareness or structures. Although they require more support through clear guidelines, outreach and training, the outreach conducted has been focused on FIs and significantly less on DNFBPs.

India is rated as having a substantial level of effectiveness for IO.11.

# Chapter 5. PREVENTIVE MEASURES

## Key Findings and Recommended Actions

## Key Findings

Financial Institutions

a) FIs generally demonstrated a good understanding of the ML/TF risks across their respective sectors, as informed by the NRA and SRA. Whilst institution-specific risk assessments are conducted, the understanding of institutional risks appears less strong, in particular for some FIs sub-sectors (cooperative banks, some MVTS providers, money changers, securities intermediaries).

b) FIs generally apply mitigating measures to a good extent. Commercial banks and some payment system operators demonstrated a stronger implementation of mitigating measures. Other FIs, including cooperative banks, some MVTS providers and money changers appear to have their ability to apply risk-based mitigation measures diminished by their less mature risk understanding.

c) The level of implementation of customer due diligence and record-keeping requirements is mixed. There are challenges on the identification of beneficial owners, in particular in more complex structures or where control is exercised by other means. The timeframe for updating high, medium and low risk client CDD information is lengthy. The Central KYC Register assists FIs maintain and track changes of information regarding their customer base. In general, FIs seem to apply EDD to domestic PEPs, notwithstanding the absence of a legal requirement, although there are inconsistencies in the breadth of domestic PEPs being identified.

d) Overall, FIs apply, to a large extent, enhanced measures for higher risk countries, new technologies, sanctions screening, and information sharing within financial groups. Most of India's FIs have adequate reporting policies and procedures. However, reporting by some sectors (non-banking financial companies, rural banks and the Department of Posts) was limited and not in line with their ML/TF risk profile. The quality of STRs has shown recent improvements but was an area of concern during most of the review period.

5

VASPs

a) Despite being brought into the AML/CFT system very recently (March 2023), VASPs generally demonstrated a good understanding of risks and obligations and started to apply CDD, EDD, and record keeping measures to a reasonable extent. The first inspections of the sector revealed challenges in the implementation of the 'travel rule' and that some VASPs did not have an adequate methodology and processes for identifying higher risk customers and applying EDD consistent with the risks. Some were in the process of integrating red flag indicators into their alert generation systems. In general, VASPs seem to conduct monitoring on an ongoing basis, which has led to the detection and reporting of suspicious transactions involving ML, predicate offences and TF.

DNFBPs

a) All DNFBP activities covered by the FATF Standards operate in India and are subject to AML/CFT obligations. However, lawyers, accountants and TCSPs are not subject to AML/CFT obligations when performing only preparatory acts.

b) Whilst DNFBPs have not begun identifying suspicious activity and submitting STRs in a significant way, the entities met on-site demonstrated a good understanding of AML/CFT obligations and ML risks, commensurate with their materiality and size of business operations, and, to some extent, TF risks. However, in the absence of supervisory findings, the assessment team cannot conclude that the positive findings from the on-site reflect the situation of DNFBP sectors more broadly.

c) Despite the lack of supervision for most DNFBPs sectors, there are some positive indications that DNFBPs apply due diligence and record keeping measures. In general, the DNFBPs met also appear to have TFS systems in place and are applying TFS requirements, although there is insufficient understanding of immediate asset freezing obligations in case of a match.

## Recommended Actions

All sectors:

a) India should address technical compliance deficiencies in relation to Recommendation 12, establishing clear obligations concerning domestic PEPs. Reporting Entities to improve identification of domestic PEPs, their family members and associates and take risk-based enhanced measures in relation to them. This could involve supervisors developing guidance tools to clarify the breath of domestic PEPs to be identified.

FIs:

a) Building on the NRA and SRA, FIs should further develop assessments of ML and in particular TF risks faced at institutional level based on the FI's own specific risk factors. This would apply to all FIs in particular cooperative banks, some MVTS providers, money changers, securities intermediaries.

b) Work with supervisors to improve FIs' ability to identify and verify beneficial owners by understanding corporate structures of clients - in particular in relation more complex corporate structures and trusts, and identification of beneficial owners based on control by other means.

c) Update CDD information on the basis of risk, and where required, shorten the time to update high, medium and low risk clients.

d) Continue improving detection of suspicious transactions, and the quality of reporting. FI sectors that are not reporting commensurate to their risks should improve understanding and controls.

VASPs:

a) Work with supervisor to enhance and update the understanding of ML/TF risks posed by VAs and different VASP activities, on the basis of an updated SRA.

b) Work with supervisors to improve risk categorisation of customers, application of EDD measures to high-risk customers and reporting of suspicious transactions, commensurate with risks.

DNFBPs:

a) Improve TF understanding through granular risk assessments of products/services, clients, delivery channels and geographical risks.

b) Apply enhanced mitigating measures for high-risk situations particularly by high-risk sectors (e.g., real estate, accountants and TCSPs);

c) Improve the understanding of implementing the TFS obligations without delay.

d) Improve detection of suspicious transactions as well as increase the quantity, diversity and quality of STRs filed by DNFBPs, particularly by high-risk sectors, when suspicious activity is detected.

e) Subject preparatory work by all TCPS, accountants and lawyers to AML/CFT obligations in line with Recommendation 22.

424. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

425. For the reasons of their relative materiality and risk in the Indian context, shortcomings in preventive measures were weighted **most significantly** for banks; **significantly** for MVTS and other financial institutions (OFIs) regulated by the RBI (which includes non-banking financial companies (NBFC), payment system operators (PSOs), authorised dealers in foreign exchange other than banks, money changers, MTTS providers etc.), VASPs, real estate agents (REAs), accountants and TCSPs (who in the Indian context include company secretaries); **moderately** for the securities

sector; and to a **limited extent** for casinos, lawyers including notaries, the insurance and pension sectors. This is explained above in Chapter 1, section 1.4.3.

426. Overall, the assessors found that:

- **Most significantly weighted**: Banks generally demonstrated good understanding and implementation of preventive measures; however, this is less developed for cooperative and rural banks.
- **Significantly weighted**: OFIs in India showed a mixed level of understanding and implementation. While many seem to implement preventive measures, some are not detecting suspicious transactions sufficiently. VASPs, REAs, TCSPs (including company secretaries) and accountants have become REs more recently. Whilst VASPs showed a more developed implementation of controls, most DNFBP sectors have yet to detect suspicious transactions and file STRs.
- **Moderately weighted**: The securities sector is generally aware of and implementing their obligations.
- **Limited weight:** Casinos, insurance and pension sectors have a reasonable understanding of their risks and implement preventive measures accordingly. Lawyers conduct activities covered by the standard to a limited extent and are not covered by obligations when performing preparatory work.

427. DPMS, as other persons, are prohibited from receiving cash payments of INR 200 000 (EUR 2222), from a person in a day or in respect of a single transaction, imposed in the Income Tax Act, which is far less than the FATF-prescribed EUR/USD 15 000. Assessors consider nonetheless DPMS the implementation of TFS obligations in IO4. Notaries are also lawyers and do not conduct activities covered by the Standard.

428. Assessors' findings on IO.4 are based on interviews with a range of private sector representatives, statistics, findings from enforcement actions provided by supervisors, and information concerning the relative materiality and risks of each sector (including the NRA and SRAs). The assessors met with a range of FIs, VASPs and DNFBPs across relevant sectors. Nonetheless, given the very large number of supervised entities, the wide diversity of the sectors, and the issues in supervision identified in IO.3, it is still difficult to generalise implementation across the sectors. This is particularly the case for sectors more recently subject to AML/CFT obligations where supervision was in a very incipient stage (e.g., accountants, company secretaries, TCSPs, real estate agents and DPMS).

## Immediate Outcome 4 (Preventive Measures)

### *Understanding of ML/TF risks and AML/CFT obligations*

*FIs*

429. Generally, FIs have a good understanding of their ML risks, with commercial banks and some payment system operators demonstrating a stronger understanding. FIs sectors have had access to a summary of the NRA's findings as well as to general and specific red flag indicators developed by FIU-IND. Generally, there has also been a reasonable level of outreach by supervisors which has contributed to a consistent understanding of the risks the India faces at a national and sectoral levels, as identified through the NRA process. However, there remains a large audience that has yet to benefit from these outreach meetings (see Immediate Outcome 1).

430. Most interviewed FIs demonstrated an understanding of ML risks in their sector. They identified, for instance, money mule accounts and trade or service-based money laundering (e.g., acquisition of software) as typical ways money is laundered through the Indian financial system and cyber frauds and other frauds (e.g., loan fraud) as common predicate offenses carried out through banks and other FIs. Banks and some other FIs participate in a public private partnership with the FIU and regulators, which is an opportunity for sharing of experience and new typologies. The typologies associated with the use of sole proprietorships or partnerships to obscure ownership or identity (e.g., in frauds and overseas remittances for ML) has also been referred to by FIs, in line with supervisory findings.

431. FIs are required to and conduct their own internal risk assessments. Despite displaying a good general understanding of ML risks identified by India at national level, some institutions (cooperative banks, some MVTS providers, money changers, securities intermediaries) showed a less nuanced understanding of their own risks at entity level, considering their own business, customer base, products and services offered and geographic footprint.

432. FIs in the securities sector demonstrated understanding the ML risks of the sector to some extent. Their perception did not fully align with the NRA findings of a medium-low residual risk. Some securities FIs were able to identify riskier areas (e.g., mutual funds, which invest funds of clients into the securities sector). Overall, securities FIs appear to be over-reliant on the sector's in-built controls (e.g., prohibition of cash transactions, reliance on the banking system), rather than developing a more nuanced understanding of their own risks.

433. Regarding TF risk understanding, all FI sectors have had access to the NRA findings on TF, with information on the different terrorist conflict areas. However, the way in which this knowledge is applied in practice varies, with some FIs appearing to be more reliant on the prescribed TFS obligations or the NRA's findings, rather than developing an understanding of their specific exposure to TF risks, on the basis of products, clients and geographic footprint. When asked about TF risks in their sector, only few FIs met on-site were able to demonstrate how they transposed their knowledge of TF risks into, for instance, controls and alerts to monitor transactions (cash withdraws, remittances, use of foreign cards) in, for example, the conflict areas referred in the NRA. One good example was an interviewed bank which, through its transaction monitoring and informed by its TF risk understanding, has been able to undercover a typology related to a foreign-sponsored scholarship funds actually destined for TF. Another good example refers to controls put in place by an FI that issues pre-paid instruments (PPIs), including wallets to monitor TF and cyber fraud risks, as summarised below.

5

### Box 5.1. Monitoring of TF and cyber-fraud risks

FI A conducts internal and external reviews to determine the nature of TF cyber threats and cyber frauds. This includes identifying both physical and digital footprint of hot spots where suspicious conduct and misuse of its instruments are observed.

In relation to TF, FI A has considered the six theatres of conflict identified in the NRA, which indicate a geographical concentration in specific identified regions. Bank A has further identified a total of 25-30 districts in India to be of high risk. Bank A closely monitors transactions originating from or directed to the risky locations.

In case of physical footprint, Bank A carries out geofencing of the user's transaction location and flags the hotspots for enhanced monitoring in terms of volume and velocity.

In case of digital footprint, Bank A app is not accessible from sanctioned countries by including them on the IP blocklist.

**1. Geo-Fencing based checks**: All the high-risk areas in a particular region are plotted into a polygon and focused controls are applied only to a targeted customers base. Transactions originating from specific locations are mapped against the polygon.

**2. Latitude Longitude based checks**: A location trial obtained from various past logins and transactions is used to determine the risk associated with the user.

**3. Machine Learning Models:** To curb the challenge of emerging hotspots, Bank A has deployed location as one of the critical parameters in various machine learning models.

**4. Scoring Algorithm:** Location is one of the key parameters in defining the risk of the customer.

Source: interviewed entity

434. FIs generally demonstrated a good understanding of AML/CFT obligations, and most of them have put in place comprehensive systems to monitor business relationships and transactions. In many cases, the systems include predefined parameters that consider red flags indicators identified by FIU-IND as well as the entity's own risk indicators (when those have been developed).

435. There are, however, concerns on the level of understanding of risks and obligations by some MVTS providers, in particular Money Transfer Services Scheme (MTSS) subagents as MTSS has been identified in the NRA as one of the main channels for TF (see next section 5.5.2 below).

*VASPs*

436. Despite being brought to the AML/CFT system very recently, VASPs have generally demonstrated a nuanced understanding of ML/TF risks and AML/CFT obligations. The understanding is enhanced by frequent and targeted communication by the FIU-IND, that also acts as VASP supervisor through extensive outreach sessions and working groups. The VASPs met on-site were informed by outcomes of India's NRA, the VASP sectoral risk assessment (SRA), their own risk assessments and international trends and patterns. However, as referenced in Immediate Outcome 3, the SRA was conducted before India regulated VASP sector for AML/CFT and as such is already outdated.

*DNFBPs*

437. In the absence of evidence (e.g., supervisory activity, STR reporting etc) on compliance levels for most of the DNFBPs owing to either the recent designation of AML/CFT supervisors for some or inadequate supervision by the existing supervisors for others, it was difficult for the assessment team to draw conclusions on the overall level of understanding of the risks and obligations beyond the entities interviewed.

438. Supervisory findings for the sector for 2022-2023 confirmed that real estate agents had generally a good understanding and developed AML/CFT policies, but some policies still required board approval or broader consideration of the NRA findings.

439. DNFBPs met on-site generally seem to have a good understanding of ML risks and AML obligations, and some understanding of TF risks and CFT obligations, generally informed by the NRA results and, in some instances, SRAs.

440. As a starting point, DNFBPs met were aware of and shared the findings of the risk assessments including sector risk categorisation. They have applied their risk assessment tools to promote an understanding of the risks associated with a suite of the products/services, customers, delivery channels and jurisdictions they offer. Documented risk assessments describe the nature and levels of risks into low, medium and high.

441. Real estate agents regarded high value developers and luxury urban homes, source of funds, PEPs and large cash transactions and concealment of property ownership through a third party (i.e., benami property) as posing higher risks. Accountants, company secretaries and lawyers rate complex company structures, shell companies and foreign beneficial owners as high-risk situations. Casinos consider cash transactions from high-risk and sanctioned jurisdictions as posing the greatest risks.

442. All DNFBPs interviewed have systems to monitor and update risk understanding at regular intervals or as and when relevant events occur. The monitoring systems have parameters for outliers for refining red flags and consider open-source information and red flag indicators from FIU-IND.

443. They generally demonstrated their understanding of AML/CFT obligations by refining mitigation measures as and when information on risk (e.g., updated NRA) was notified and domestic AML/CFT change (e.g., downward revision of BO percentage), although a smaller CSP had a limited understanding of BO. The understanding of the nature and the level of the ML/TF risks seem influenced by the NRA findings, though TF risk understanding at granular level remains a challenge.

444. Notwithstanding, the situation across DNFBP sectors beyond interviewed entities may be less positive. As noted under Immediate Outcomes 1 and 3, whilst the NRA findings have been communicated to the many DNFBPs across different states via an outreach exercise that took place recently, there remains a significant number of reporting entities that have not been engaged. There has neither been sufficient outreach nor sufficient compliance checks in respect of AML/CFT obligations. More broadly, the very small number of STRs filed raises questions on the level of understanding and application of AML/CFT obligations across DNFBP sectors.

### *Application of risk mitigating measures*

*FIs*

445. FIs apply mitigating measures to a varying extent. Larger banks and more technology driven FIs, including large MTSS overseas principals, have more comprehensive procedures and

demonstrated a stronger application of risk mitigating measures. The supervisor collects detailed information on banks and larger FIs' controls and found that the sector generally has comprehensive AML/CFT policies adopted by senior management. Several examples of mitigating measures were shared during the on-site. For instance, most FIs do not rely on customer due diligence performed by third parties and only carry their own; they submit all new customers to sanctions screening and run their customer database against the lists regularly; they would onboard PEPs after approval from senior management. Some banks would still only open accounts face-to-face; and for corporate customers, some would do field verification and in-person meetings with management; others have established video onboarding for their non-face-to-face businesses.

446. One area where FIs require improvement is the risk profiling of customers, which has been a supervisory concern for the last two years. Supervisory findings identified that the risk profiling matrix of some FIs was not extensive or precise enough to capture the 'true' risk of clients. Larger banks appear to have more robust procedures in this regard. However, some FIs do not appear to have procedures in place to risk rate their products and services and only risk rank clients.

447. Some of the other FIs, including cooperative and rural banks, as well as certain FIs in the foreign exchange market, have their ability to apply risk-based mitigation measures diminished by their less mature risk understanding. MTTS providers rely on agents and subagents some of which have less mature risk understanding and, in turn, a diminished ability to implement risk-based mitigation measures. For instance, a large MTSS overseas principal, shared that out of all markets it operates, it has the highest turnover of subagents in its India operations, due to failures in complying with AML/CFT requirements leading to the termination of the relationship with over nine thousand agents from January 2018 to October 2023. RBI has also imposed sanctions on agents due to AML/CFT failures related to their subagents as well as directed various MTSS agents to undertake audit and inspection of their sub-agents in the frequency specified in guidelines.

448. The legal requirements provide that Overseas Principals are fully accountable for the actions of their agents and sub agents in India. However, they do not go as far as requiring principals or agents in India to include their agents and subagents, respectively, in their AML/CFT programmes and monitor them for compliance with these programmes, as required by the FATF. In relation to FIs in India's international finance centre (IFSC), all banks and many other FIs are branches of other FIs operating in India or other countries and as such have been implementing mitigation measures over time. It is difficult to assess whether they have been implementing mitigating measures commensurate with the specific IFSC risks.

*VASPs*

449. Despite VASPs only being incorporated into the AML/CFT framework in March 2023, interviewed VASPs demonstrated having integrated risk-based mitigation measures into their operations. This includes applying enhanced controls to help mitigate VA specific risks, including transaction monitoring and dynamic risk re-evaluation of customers. Specific additional parameters for customer risk categorisation including defining IP risk score, digital identity score, transactional volumes, inbound cybercrime queries, and overall account transaction velocity score. Interviewed VASPs indicated that high-risk clients undergo a video KYC process, enhanced transaction monitoring, and additional independent verification of employment or source of income. FIU-IND supervisory findings indicated that some VASPs were yet to develop a methodology and processes for identifying higher risk customers and applying EDD to them. Some were in the process of integrating of red flag indicators into their alert generation system.

*DNFBPs*

450. There is some data for real estate agents and casinos, and none for other DNFBPs, on supervisory actions that would allow an appreciation of DNFBPs' ability to apply mitigating measures that are proportionate to their risks and size, to draw up concrete conclusions. Inspections findings on real estate agents indicate that most inspected entities apply mitigating measures. Some did not demonstrate a full understanding of the red-flag alerts shared by FIU-IND, while most understood and were analysing them.

451. Despite being in the early stages of AML/CFT supervision, the DNFBPs interviewed apply mitigating measures on products and services, clients, delivery channels and jurisdiction determined through entity risk assessments. More specifically, mitigating measures are generally applied on a case-by-case basis in the sector since most of the products and services are for walk-in clients, with casinos using loyalty programs to enhance their application of the measures as risks changes.

452. While DNFBPs indicated that they have clients and transactional assessment tools that are used to identify and monitor client profiles for applying commensurate controls, their implementation varies. Real estate agents and casinos are more advanced in their application of risk-based due diligence measures compared with professionals, seemingly due to lack of AML/CFT supervision.

### *Application of CDD and record-keeping requirements*

*FIs*

453. FIs generally apply CDD and record-keeping requirements and have procedures in place for identifying customers and systems for ongoing monitoring. FIs interviewed refuse to open an account or conduct a transaction if they are unable to complete CDD. FIU-IND has applied monetary penalties to at least six FIs for failures to conduct CDD when opening accounts during the review period. Compliance appears to be improving since then.

454. One important development in this area is the implementation of Central KYC Registry (CKYCR), hosted by the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI). FIs are required to submit some CDD information, including customer name, address, ID and tax registration number, authorised signatories and beneficial ownership information for all account-based relationships they establish with individuals since 2017 and with legal persons or arrangements since 2021. In addition, when FIs update the CDD records of an account-based relationship established before 2017/2021, they are also required to add information in relation to those accounts in the Registry, which will ultimately lead to the inclusion of all active accounts in the CKYCR. At as November 2023, the Registry contained records of over 803.23 million individuals and 1.896 million non-individual accountholders (companies, LLPs, trusts, societies etc).

455. The CKYCR issues a unique KYC Identifier for each customer, which links that customer to accounts it may have with different FIs. When a FI reports a change in the CDD information of a customer, the Registry sends an electronic notification of the update to all FIs which have recorded the same customer in the Registry. This is a powerful tool enabling FIs to keep track of changing of information regarding their customer base (see analysis in Recommendation 10, c.10.3) and identify discrepancies. In its supervisory letter in February 2023 RBI urged banks to resolve pendency in relation to updating the Registry and has since monitored progress. As at September 2023, 7.2% of accounts considered high-risk had not yet been registered in the CKYCR, however,

on the whole, only 0.52% of the total universe of bank accounts remained unregistered in the CKYCR at that point.

456. On transaction monitoring, RBI's guidance on the maximum timeframe for updating customer's CDD information for high, medium and low risk clients, is set at two, eight and ten years, respectively. This does not ensure timely updates (see c.10.7). Some banks adopted lower timeframes, but that would not be the case for all banks and all other sectors.

457. The requirements regarding identification of beneficial owners do not appear to be fully understood or implemented across all sectors. Some FIs demonstrated understanding the need to identify and verify BO information and they have procedures in place to do so. However, BO identification seems more reliant on ownership. The requirements for identification of BO in case of control by other means or more complex corporate structures seems to represent a challenge for many FIs. Inspections from RBI and SEBI, banking/MVTS/OFIs and securities supervisors respectively, revealed that identification and verification of beneficial owners remains a challenge for FIs. BO identification was one of the major deficiencies identified by RBI from inspections of commercial banks, while CDD/KYC failures was on the main violations found in inspections of (non-bank) foreign exchange dealers. India's 2023 Action Plan also identifies the need for payment intermediaries to ensure compliance with CDD requirements.

458. For the identification of the beneficial owners of Indian legal persons, FIs heavily rely on the information available in the MCA registry. It remains unclear how well FIs understand the customer's ownership and control structure and the beneficial owners they are required to report. FIs interviewed did not mention instances where they have identified the beneficial ownership by means other than control through ownership interests, although a couple of case studies have been provided demonstrating that some FIs have been able to identify BOs even in complex structures.

459. Interviewed FIs also identified challenges identifying the beneficial owners of trusts, sole proprietorships, general partnerships as well as foreign legal persons and arrangements, because there is no central registry like the MCA registry where beneficial ownership information can be consulted. This appears to demonstrate a narrow approach to conducting CDD. One of the typologies identified in recent years refer to the misuse of bank accounts of sole proprietorships and general partnerships for fraud and cyber-fraud in India, as highlighted by the bank supervisor. It is not clear if CDD of all FIs had been sufficiently robust enough to identify persons excising control or acting on behalf of the customer.

460. Some interviewed FIs noted that there would be locks in their systems to prevent opening accounts when beneficial ownership information has not been identified. In addition, one large bank noted having procedures to deal with discrepancies between beneficial ownership information available in public sources and the CDD information collected by the bank. Those cases would be escalated to a controller within the bank and a decision would be taken on whether there the situation is suspicious and should be reported. Most interviewed FIs did not indicate that they have or would consider reporting discrepancies of beneficial ownership information to the MCA or other authorities. However, FIU-IND noted that discrepancy between CDD and MCA records is a red-flag indicator and should lead to the filing of STRs. During the review period, there has been 119 STRs about discrepancy in BO information.

461. India has developed a number of financial inclusion products including the concept of small accounts (see c.10.3). Those are free-of-charge accounts whose balance cannot exceed INR 50 000 (EUR 562) at any point in time and can be opened by any person by signing or adding a thumb print to a self-attested photograph. Those accounts provide access to basic financial services for persons who normally could not afford the costs of regular accounts and who may not have an officially issued ID. One interviewed bank which had a strong focus on financial inclusion products, noted

that it is currently rare for persons not to present an official ID (Aadahar card) to open an account and that small accounts are now being opened with full ID information. Some small finance banks that operate in rural areas and target low-income clients also act as Aadhaar enrolment agents and can assist customers with obtaining their ID card. A public sector bank indicated that small accounts represent approximately 20% of its accounts and that they monitor accounts for any money mule risks (despite the low balance permitted). Most private sector banks indicated having very few small accounts in their portfolio.

*VASPs*

462. VASPs met during the onsite had a good understanding of their CDD and record keeping obligations. The two on-site inspections conducted by FIU-IND confirmed these VASPs are generally applying CDD and record keeping requirements. These on-sites also revealed some issues for remediation including risk categorisation of customers, and processes for identifying higher risk customers. Considering the non-face-to-face nature of the business, VASPs are focused on collecting additional CDD information, such as details of a bank account in the name of the customer (verified through a 'penny drop'[102]), check the customer's ID information against databases[103], a registered phone number (one-time password sent to the phone, verification of registered owner with a database), device international mobile equipment identity and associated IP address. VASPs met verify whether the name and other credentials match across all data points; if not, they do not accept the customer. They take additional CDD measures, for instance one VASP undertakes a video call and request information on source of funds for transactions above a certain threshold (USD 2 000). VASPs refuse business if CDD is incomplete. However, as supervision is recent, it is not possible to confirm the level of compliance for the entire sector, although indications from offsite monitoring confirm good understanding and compliance with obligations.

*DNFBPs*

463. DNFBPs seem to understand their obligations for applying due diligence and record keeping measures on business relationships and transactions, although implementation varies. In the real estate sector, supervisory findings show that most supervised entities comply with AML/CFT obligations, though some challenges were identified for CDD (for customers onboarded prior to 2022) and BO identification in some entities.

464. The DNFBPs interviewed indicated that business relationships and transactions can only be concluded when CDD measures are met and they have satisfied themselves when there is doubt about the veracity of the CDD information obtained. By contrast, such decisions are not taken when there is insufficient or incomplete or doubtful CDD information. However, there is no conclusive evidence that filing of STRs is considered by the DNFBPs interviewed when there is incomplete CDD information given that there has been very few STRs filed by the sector (i.e., 10) during the period under review.

465. DNFBPs interviewed collect basic due diligence information (national identity, company incorporation and ownership information and address) for all risk situations. EDD is performed for high-risk clients and transactions. This includes requesting the client for additional information which is subjected to enhanced scrutiny to satisfy the CDD procedures prior to beginning a business

[102] Penny drop verification is a method used for validating a bank account, which involves depositing a small amount of money (e.g., EUR 0.01) into the account. This process serves not only to authenticate the customer's bank account but also to confirm that the account is active. Moreover, it helps to establish whether the provided account details belong to the same person or not.

[103] From the Central Economic Intelligence Bureau and National Crime Records Bureau.

relationship or concluding a transaction. For instance, real estate agents and professionals collect and verify BO information above 10 percent as per the domestic requirements, although professions engaged in company formation services have indicated facing challenges in verifying foreign BO but have taken reasonable measures to verify them, such as obtaining notarised records. Real estate agents apply full due diligence measures on natural persons and real estate development companies and obtain information on promoters, directors and BOs prior to processing a transaction.

466. For record keeping obligations, the DNFBPs interviewed indicated that they go beyond the AML/CFT legislation by also adhering to other statutory requirements such as tax and company formation. DNFBPs typically keep records in both electronic form and hard copies for a minimum of five years following termination of a business relationship and a transaction, and these records have been accessed by FIU-IND, supervisors and LEAs upon appropriate request.

### *Application of EDD measures*

#### *Politically Exposed Persons (PEPs)*

467. FIs, VASPs and DNFBPs interviewed described the measures in place to identify PEPs, foreign and domestic, as well as the EDD measures applied in these cases (including obtaining senior management approval), despite the lack of obligations and guidance in relation to domestic PEPs. FI supervisors considered that this would be the case for the entire sector but did not provide evidence.

468. Larger FIs as well as reporting entities met on-site do appear to rely on group wide policies meaning that they are automatically treating domestic PEPs as high-risk and conducting EDD, as well as foreign PEPs as required, using commercial software to help identify PEPs when conducting CDD. Some reporting entities rely on self-declaration for the identification of both PEP and close associates, while others would also rely on public sector databases (e.g., electoral commission). There are also some inconsistencies on the breadth of domestic PEPs being identified (e.g., whether PEPs in local or state levels are being identified).

469. The identification of domestic PEPs and the application of enhanced measures to them remains an area of concern, in view of the lack of legal or regulatory requirements, with the exception of the guidelines issued for entities regulated in the international financial services centre (see R.12). Clarifying the preventive measures applicable in this context would be crucial in India's risk and context, considering the threats associated with corruption and bribery are among the highest in the country, as identified in the NRA.

#### *Corresponding Banking*

470. Banks generally have well defined correspondent banking policy, involving a detailed assessment of respondent bank (for example, gathering details about the beneficial owner and the board of directors, sanction screening them, media searches), board approval for new corresponding bank relationships, ensuring the respondent bank holds a valid license, and assessing its AML/CFT policy. RBI, the banking supervisor, did not identify violations by FIs of their obligations in connection with correspondent banking relationships during the review period. FIs also provide statistics concerning their corresponding banking relationships to RBI on a quarterly basis.

*New technologies*

471. All reporting entities are required to carry out a risk assessment to identify, assess and take effective measures to mitigate ML/TF risks in connection with new products or business practices, including new delivery channels. Risk assessments need to be documented, consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied, be kept up to date and be available to regulators and competent authorities.

472. FIs are aware of these obligations and only launch products after approval by their risk management structures (generally at board level and/or by compliance departments), as also confirmed by interviews and the regular reviews by the RBI. FI Regulators also allow regulatory sandboxes for the live testing of new products or services in a controlled environment. For instance, one interviewed FI that provides pre-paid instruments, including digital wallets, which are subject to minimal CDD (see c.10.3) developed monitoring tools to mitigate TF risks, including geo-location in line with the TF geographical theatres identified by the authorities, as well as, for online customers, trolling websites to identify goods and services being sold/acquired.

473. India has witnessed the rapid pace of emergence of new products, services, and business models, in particular in the financial sector. This includes various categories of payment intermediaries (including aggregators and gateways), digital wallets, automated stock advisory services, VASPs, and peer-to-peer lending platforms. These new offerings are often referred to collectively as fintech.

474. Part of the fintech sectors including VASPs, payment gateways and digital wallet providers that have been more recently incorporated to the AML/CFT framework.

475. One of the main ML/TF risks identified in the NRA in respect of fintech is the potential misuse of fintech apps with poor regulatory compliance for ML, with subsequent fund off-take in virtual assets through VASPs with low AML/CFT compliance.

476. The sector has been subject to closer engagement by the authorities. One fintech company has recently been sanctioned for challenges related to non-face-to-face business and monitoring of customers from foreign jurisdictions (see case in chapter 6.2.5 below). The case below illustrates how an issuer of pre-paid instruments (PPI) conducted a risk assessment prior to introducing new features to its products:

### Box 5.2. New Feature in a PPI product

A RE introduced interoperability on its pre-paid instruments (PPIs) in Q2-2022. With this, customers can transfer money to any bank account or any Full CDD PPI across the country using Unified Payment Interface (UPI) network. Additionally, the customers can also use their Full KYC PPI to transact at any merchant across the country.

Prior to introducing these additional product features, the issuer undertook an AML risk assessment of the product. It observed that the new feature led to an increased boundary where customers could utilize their balance, not only with merchants onboarded by the RE, but also with merchants onboarded by any other FI. As part of the launch, the issuer introduced additional transaction monitoring rules. The RE also reviewed the other existing controls and product features which mitigate this risk. These include: customer type (individual customers residing in India and Indian citizens), transactions limits (monthly load limit, outstanding balance limit), product features (no cash withdrawal, no cross-border transactions) and based on which the residual risk was considered to be not very significant.

Source: RBI

*Wire transfer rules*

477. FIs conducting wire transfers demonstrated being able to apply mitigating measures for domestic and cross-border wire transfers, to ensure that funds transfers are accompanied by information on the payer and payee and have policies in place to reject wire transfers where information is incomplete or when there are AML/CFT concerns. This is consistent with RBI's supervisory findings. During its inspections in the review period, RBI identified very few institutions that failed to comply with wire transfer rules (two banks per year in the first three years of the review period, then one for the fourth year and none for the fifth year).

478. In India, FIs are required to provide cross-border wire transfer reports to FIU-IND in relation to all cross-border wire transfers of the value of more than INR 500 000 (EUR 5 580) or its equivalent in foreign currency where either the origin or destination of fund is in India. This provides FIU-IND with visibility of the extent to which these transactions are being reported, including information on the parties to the transactions. During the review period, FIU-IND fined four banks for failure or incorrect filing of these reports, which demonstrated that FIU-IND is closely monitoring compliance in this respect.

479. Interviewed VASPs and the VASP supervisor (FIU-IND) confirmed that VASPs in India are implementing technological solutions to comply with the travel rule. At the time of the on-site, 18 VASPs had implemented such technological solutions; 9 VASPs did not perform VA transfers and therefore were not required to implement the travel rule. One VASP was found to be not implementing the travel rule and compliance action has been initiated by FIU-IND. VASPs are receiving and submitting counterparty information from/to other VASPs which are on the same travel rule solution. However, the "sunrise issue" – i.e., the period where travel rule enforcement is staggered globally – is a challenge for VASPs, as they do not always receive of data/response from all originator/beneficiary VASPs. This is due to lack of travel rule implementation in some jurisdictions or differences in regulation (e.g., different thresholds established). Other challenges VASPs are facing with the travel rule implementation include issues with counterparty

identification,[104] interoperability between travel rule providers,[105] handling non-compliant deposits,[106] different data protection laws,[107] and delay in receipt confirmation from the counterparty VASP.[108] Until the sunrise issue and other issues are resolved, the Indian sector has deployed a self-declared format to collect and hold data; however, this does not fully address the challenges.

*Targeted financial sanctions (TFS)*

480. FIs and VASPs demonstrated good awareness of TFS obligations and use TFS screening software to automatically screen onboarding and existing customers as well as transactions against all relevant lists, including UNSCR lists, on a daily basis. FIs and VASPs generally appear to use software developed by third-party providers, which is also subject to continuous updates. This is consistent with supervisors' findings in respect of commercial banks and VASPs. To date, FIs and VASPs have not identified any positive matches, but many false positives.

481. DNFBPs demonstrated a reasonable understanding of the UNSCRs TFS freezing obligations and applied the CDD procedures. Most real estate agents that had been inspected implemented TF TFS, whilst few had not done so. All DNFBPs interviewed developed and implemented written and automated procedures and systems (e.g., subscription to commercial screening databases) on steps to be followed on receipt of the list from the authorities, receiving notifications of updates to the UNSCR list directly and screening it against their clients and transactions immediately (i.e., before receiving the same from the authorities). When there is a positive match, all DNFBPs met on-site understood the obligation to immediately report to the authorities as per the regulations but vary on the understanding of the timing to freeze assets. Some DNFBPs (regardless of size) indicated that if they were to find a positive match, they would not freeze the asset unless they have notified and received instruction from FIU-IND to do so which is likely to undermine the freezing without delay obligation. The mixed understanding could be attributed to low supervisory coverage including provision of specific guidance and outreach activities as well as the lack of compliance checks and clarity of the freezing requirements themselves (see IO.10 and R.6). In practice, no match was found to demonstrate effectiveness of the TFS measures by the DNFBPs during the period of the review.

*High risk jurisdictions*

482. FIs understand the obligation to apply EDD to business relationships with a nexus to a high-risk country or jurisdiction and have procedures in place to do so. In practice, the interviewed entities adopted a broad approach to assessing and mitigating jurisdictional risks, typically relying

[104] Since there is no publicly verifiable database which lists the central wallets of all VASPs, it becomes difficult to accurately ascertain if originator/beneficiary wallets are central wallets of VASPs or un-hosted wallets.

[105] Due to the lack of interoperability between travel rule providers, there is no single network which currently supports communication between all VASPs

[106] There are no mechanisms between VASPs to stop and return travel rule non-compliant deposits.

[107] Since different geographies have different local data protection laws, transmitting customer information across geographies raises concerns about local data protection requirements.

[108] Travel Rule compliance requires that the travel rule data be sent along with the transaction and the confirmation of such transactions should happen in real-time. However, as per the current workflows, the beneficiary VASP receives the travel rule data transfer post the transaction is completed on the blockchain. In some cases, even days after the transaction is completed on the blockchain. Similarly in case of VA withdrawal requests, the counterparty VASP takes time to respond to the travel rule data transfer.

on (a) guidance from the authorities, in particular FIU-IND, (b) the FATF ICRG List, (c) international or regional organisations, (d) automated reliable and widely used commercial databases and (e) own institutional risk assessments. The lists are accessed directly from the websites of the concerned organisations from which the information obtained is fed into the screening and risk assessments tools for analysis of the risk profiles and application of EDD. The same was found in relation to VASPs and DNFBPs interviewed.

483. In relation to FIs supervised by the RBI, during the review period, there was only a small number of occasions where RBI found shortcomings in FI's compliance with EDD requirements, which seem to confirm a good level of implementation including the requirements on high-risk countries. FI procedures may vary depending on the jurisdiction.

484. In relation to DNFBPs, some of the entities with foreign ownership (e.g., real estate agents and casinos) indicated that they also used the systems of the group to apply EDD measures against situations from high-risk jurisdictions. There were no supervisory findings to confirm the broader compliance by VASP and DNBFP sectors in this regard.

### *Reporting obligations and tipping off*

485. FIs and VASPs met on-site were aware of their STR reporting obligations, identifying suspicious activity and submitting increasing numbers of STRs to FIU-IND in most sectors. Public and private commercial banks were responsible for the majority of STR filing during the review period (68%), followed by payment banks (11%). The VASP sector is taking steps implementing reporting obligations since becoming REs in March 2023 and this has already generated the dissemination of eight operational analysis reports by the FIU, seven in relation to ML and one for TF. On-site inspections of VASPs reveal some issues with STR filings, which were followed-up with the VASPs involved.

486. Some FI sectors do not appear to be reporting commensurate to their risk and volume of transactions. For instance, the level of reporting by NBFCs, a sector that constitutes approximately 10 000 entities, appears to be low. NBFCs are deposit-takers and lenders, and the total number of reports filed by the sector, approximatively 8 000, represents less than one STR filed per entity in the entire review period. There has been a negligible number of STRs filed by entities in the IFSC. At the time of the on-site, there were still some IFSC FIs that had not registered with FIU-IND and were unable to file an STR in the FIU portal. The Department of Posts (DoP), which provides both MVTS (as an MTSS agent) and banking services across India, filed 182 STRs in the first year of the review period, and only eight STRs in total for the following four years. The number of STRs from full-fledged money changers and authorised dealers in foreign exchange also appear relatively low, even if some of their activity may be considered of lower risk in comparison with other FIs. One of the main deficiencies from 2022/2023 RBI inspections in authorised foreign exchange dealers was the inexistence of a system to generate alerts for transactions or alert generation inconsistent with risk. FIU-IND enforcement action in cooperative, public and private banks and other FIs also indicated failures in these institutions (see section 6.24 in Immediate Outcome 3), which were later remediated.

487. FIs have procedures for reviewing alerts and decide whether the activity is suspicious, including established timeframes. Timeframes seem to vary significantly by FI, while some indicated trying to clear alerts in a very short timeframe (two days), others indicated needing 45-60 days for simpler issues, and more for more complex cases. As a result, not all FIs may be submitting STRs promptly as required. Overall, alert management issues, including generation of alerts, review and closure, and time taken for processing the alerts is still a common violation found by the RBI in inspections of commercial banks, NBFCs and UCBs.

488. STR reporting in year 2020-2021 appear to have been negatively affected by the COVID-19 pandemic. Although the number of alerts increased for most FIs, some stopped sending STRs for some time during the pandemic. STR filing has increased in the following year, which may indicate that some transactions were being reviewed at that time. One interviewed bank reported pausing its alert generation for some time during the pandemic, which would have impeded it from monitoring suspicious transactions during that period.

### Table 5.1. Sector-specific Data on Filing of STRs

| Sector | Sector Subcategory | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 | 2023-24 (until 22 Nov 2023) |
|---|---|---|---|---|---|---|---|
| Banks | Public Sector Banks | 96 434 | 106 179 | 47 961 | 103 151 | 187 394 | 80 290 |
| | State & District Co-Operative | 15 | 55 | 79 | 142 | 223 | 70 |
| | Private Sector Bank | 63 971 | 92 787 | 62 086 | 76 954 | 97 823 | 51 805 |
| | Small Finance Banks | 695 | 2 266 | 4 424 | 5 388 | 9 579 | 8 274 |
| | Regional Rural Banks | 7 | 106 | 64 | 96 | 247 | 17 |
| | Urban Cooperative Banks | 12 336 | 18 399 | 32 707 | 51 319 | 29 586 | 4 779 |
| | Payment Banks | 1 374 | 18 718 | 42 809 | 40 079 | 50 503 | 13 310 |
| | Other Banks | 3 301 | 3 651 | 4 664 | 7 199 | 10 375 | 14 158 |
| NBFCs | | 414 | 556 | 986 | 1 984 | 3 101 | 1 756 |
| Insurance | | 2 779 | 2 253 | 2 028 | 6 452 | 5 590 | 2 402 |
| Housing Finance Companies | | 44 | 261 | 157 | 35 | 227 | 82 |
| Money Transfer Service Scheme | | 1 643 | 5 800 | 4 138 | 5 334 | 3 665 | 569 |
| Money changers | | 20 | 175 | 92 | 549 | 114 | 482 |
| Dept of Posts | | - | 182 | 2 | 2 | 4 | - |
| Capital Market Intermediaries | | 3 758 | 3 588 | 3 946 | 6 966 | 9 151 | 2 495 |
| PFRDA Intermediaries | | 144 | 1 | 15 | 18 | 126 | |
| Casinos | | - | - | 1 | - | 1 | 4 |
| VASP Sector | | - | - | - | - | - | 837 |
| IFSCA FIs and DNFBPs | | 1 | - | 1 | 1 | 4- | 6 |
| Real Estate Agents | | - | - | - | - | - | 4 |
| TCSPs | | - | - | - | - | - | 2 |
| Accountants and Lawyers | | - | - | - | - | - | - |
| Others (Prepaid Instruments Issuers, Payment Aggregators, Card System Operator, OPGSPs etc) | | 574 | 3 626 | 8 783 | 2 833 | 13 402 | 2 294 |
| Total | | 187 509 | 258 603 | 214 942 | 308 501 | 421 111 | 183 633 |

Source: FIU-IND

489. The quality of STRs had been area of concern across different financial sub-sectors over the review period, with recent improvement. There is also a mechanism for incoming STR quality control which rejects reports that are lacking necessary attributes and follows up with the reporting entity to rectify the deficiencies for it to be resubmitted. In volume, most rejected STRs were filed

by public and private commercial banks (4% of total STRs) and cooperative banks (8%). In relative terms, small finance banks had 10% of their STRs rejected by the FIU. FIU-IND has closely engaged with FIs, providing feedback on STRs filed, requesting resubmission of rejected STRs and applying financial sanctions on egregious situations. Regulators have been also working with their sectors to increase STR reporting and improve their quality. This engagement is likely to have played an important role in the significant improvement over time across most sectors, as the reduction in the percentage of rejected STRs seem to indicate (from 15% in the beginning of the review period to 0.3% towards the end).

5

490. Most compliance actions for failure with reporting obligations taken by FIU-IND from 2018 to November 2023 were against cooperative banks (46%), followed by public sector banks (17%). India indicates that the banks which were penalised for failure to file STRs or other reports have since rectified their systems and procedures and now comply with the reporting obligations.

### Table 5.2. Rejected and Refiled STRs by Sector

| Sector | Sector Subcategory | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 | 2023-24 (until 22 Nov 2023) | Total |
|---|---|---|---|---|---|---|---|---|
| Banks | Public Sector Banks | 20 526 | 1 948 | 1 764 | 837 | 140 | 35 | 25 250 |
| | State & District Co-Operative | 7 | 16 | 15 | 11 | 7 | 3 | 59 |
| | Private Sector Bank | 1 100 | 10 484 | 3 665 | 1 553 | 335 | 41 | 17 178 |
| | Small Finance Banks | 557 | 734 | 737 | 721 | 348 | 87 | 3 184 |
| | Regional Rural Banks | 2 | 9 | 18 | 20 | 4 | 2 | 55 |
| | Urban Cooperative Banks | 3 266 | 2 745 | 2 691 | 3 384 | 929 | 320 | 13 335 |
| | Payment Banks | 21 | 5 | 18 | 10 | 2 | 1 | 57 |
| | Other Banks | 777 | 1 655 | 336 | 467 | 83 | 7 | 3 325 |
| NBFC | | 132 | 25 | 26 | 34 | 16 | 4 | 237 |
| Insurance | | 238 | 273 | 60 | 20 | 8 | 5 | 604 |
| Housing Finance Companies | | 11 | 2 | 2 | 2 | 5 | - | 22 |
| MTSS | | 31 | 53 | 92 | 214 | 26 | 7 | 423 |
| Money Changers | | 8 | 24 | 10 | 5 | - | - | 47 |
| Dept of Posts | | | | | | | | |
| Capital Market Intermediaries | | 217 | 86 | 28 | 20 | 3 | 1 | 355 |
| PFRDA Intermediaries | | - | - | - | - | - | - | - |
| VASP Sector | | - | - | - | - | - | - | - |
| IFSCA FIs & DNFBPs | | - | - | - | - | - | - | - |
| DNFBPs | | - | - | - | - | - | - | - |
| Others (PPIs, Payment Aggregators, Card System Operators, OPGSPs etc.) | | 30 | 13 | 18 | 574 | - | - | 635 |
| Total | | 26 923 | 18 072 | 9 480 | 7 872 | 1 906 | 513 | 64 766 |

Source: FIU-IND

**Table 5.3. Data on STRs Filed, Rejected and Refiled**

| | FY2018-19 | FY2019-20 | FY2020-21 | FY2021-22 | FY2022-23 | 2023-24 (until 22 Nov 2023) | Total |
|---|---|---|---|---|---|---|---|
| Valid STRs filed by FIs | 187 509 | 258 603 | 214 941 | 308 501 | 421 110 | 182 786 | **1 573 450** |
| Valid STRs filed by DNFBPs | 0 | 0 | 1 | 0 | 1 | 8 | **10** |
| Valid STRs filed by VASPs | | | | | | 837 | **837** |
| STRs Rejected | 26 923 | 18 072 | 9 480 | 7 872 | 1 906 | 513 | **64 766** |
| STRs Refiled | 26 923 | 18 072 | 9 480 | 7 872 | 1 906 | 513 | **64 766** |

491. Interviewed FIs and VASPs were aware of their obligation to avoid tipping off customers when they file a STR. They take a number of practical measures to prevent tipping off, depending on the organisation or structure of the firm. Measures include: contractual confidentiality obligations with employees or with outsourcing companies; company rules for employees and management (e.g., code of conduct); and training, and, for some larger entities, specific procedures to collect information about the customer without informing branches or officers with a direct customer relationship. Some FIs maintain alert management systems and STRs centrally and do not share this information with their local branches, i.e., the entities that hold a direct relationship with the customer.

492. In relation to DNFBPs, the total number of STRs filed (10 STRs in during the period under review) is disproportionately low, especially for real estate agents, accountants and TCSPs, the higher risk sectors. As indicated in Chapter 1, at the time of the on-site a very small number of DNFBPs were registered with the FIU (e.g., 144 real estate agents, 36 TCSPs, 120 accountants) which indicates that only a very small percentage of the sectors were ready to report. The low supervisory coverage during the review period is likely to be the major contributor to the low STR levels.

493. Notwithstanding, the DNFBPs met on-site seem to have a good understanding of obligations regarding suspicious transactions reporting and tipping off prohibition for ML and TF. They indicated that they have systems for transactions detection and procedures for escalating internal suspicious transactions and processes for reporting them to FIU-IND. The interviews further revealed that staff are trained on tipping off requirements and no breaches have occurred. It remains, however, that the very low level of STR reporting by DNFBPs raises question on the level of understanding and application of STRs obligations particularly in the absence of adequate supervisory action.

### *Internal controls and legal/regulatory requirements impending implementation*

494. FIs understand the obligation to apply group-wide AML/CFT policies and do so in practice, as confirmed by supervisory findings. The information that they effectively share at group level has been limited to general risk assessments and trends, auditing reports, significant findings and outcomes of the risk assessment processes. Some FIs do not share specific client data with group entities overseas. India recently brought the legal requirements on group-wide policies in line with the standard,[109] and that may assist FIs expanding information sharing as well as applying appropriate additional measures where required.

[109] In October 2023, the amendments to the PML Rules clarified that every reporting entity, which is part of a group, are implement group-wide programmes against ML and TF, including group-wide policies for sharing information required for the purposes of CDD and ML and TF risk

495. Despite the nascent AML/CFT supervision, there are indications that DNFBPs adopt AML/CFT compliance programmes to mitigate and manage risks based on their ML/TF risk understanding, the size and business activities. There is mixed implementation of the measures as shown by the real estate agents and casinos further advanced compared to accountant and company secretaries. This situation is likely due to the insufficient supervisory coverage following the recent AML/CFT designation of SRBs for monitoring compliance by these professionals. Further, the DNFBPs indicated having internal and external audit structures for AML/CFT assurance and mechanisms in place to use the audit findings for staff training (e.g., casinos) and adjustment of their compliance programmes. Additionally, a casino upgraded its CDD measures by acquiring facial recognition software to address enhance CDD measures following audit concerns. The DNFBPs interviewed with international nexus implement home-host requirements and applied proportionate mitigating measures for treatment of the risks posed by high-risk and sanctioned jurisdictions. For instance, real estate agents engaged in cross-border transactions subject domestic PEPs to home AML/CFT obligations even though it is not a legal requirement in India.

496. The FIs, VASPs and DNFBPs interviewed had their AML/CFT policies and procedures approved by the boards or similar structures and reviewed regularly. They have appointed senior compliance officers who are supported by teams and report to their boards and liaises with the FIU-IND and other authorities. Further, they indicated that they have internal and external audit structures for AML/CFT. Also, they implemented integrity checks on employees before and during employment such as conducting background checks on educational qualifications, criminal and previous employment records and residential address. Negative findings from the checks result in rejection and termination of employment. Training is ongoing, tailor-made, and updated. For FIs, the bank and MVTS supervisor has noted the increased need for training of FI staff across different sectors, but in particular for NBFCs, UCBs and MVTS (FFMCs and foreign exchange dealers).

497. In relation to DNFBPs, real estate agents, casinos and DPMS interviewed used red flags from the FIU-IND and NRA findings to train frontline staff on identification of large cash transactions and splitting of winnings while senior management were appraised on changes to recently revised AML/CFT guidelines for the sector. To some extent, professionals including accountants and company secretaries (a type of TCSP) applied similar measures but require closer supervision which is expected given the recent designation of their SRBs as AML/CFT supervisors.

498. There are no legal or regulatory requirements in India impeding the implementation of AML/CFT requirements for FIs, VASPs and DNFBPs.

management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off (section 3A).

## Overall conclusions on IO.4

In the financial sector, there is a good general understanding of risks and obligations as well as application of mitigating measures, in particular by commercial banks, which are weighted most heavily, but less so for some OFIs in the foreign exchange sector, cooperative banks and securities intermediaries. CDD and enhanced measures are being applied but the identification of beneficial owners is an area for improvement. All sectors seem to apply EDD to domestic PEPs, notwithstanding the absence of a legal requirement, but there are some inconsistencies on the breadth of domestic PEPs being identified.

Despite the nascency of AML/CFT supervision and obligations for VASPs and DNFBPs, there are some positive indications of implementation of preventive measures. VASPs generally demonstrated a good understanding of risks and obligations and seem to apply preventive measures to a reasonable extent. DNFBP sectors met onsite seem to be developing a good understanding of their risks and obligations and applying preventative measures to a reasonable extent, but this could not be demonstrated for most DNFBPs, including some higher risk sectors, due to the limited supervision in place.

There are also major shortcomings in some sectors' compliance with reporting obligations. Suspicious transaction reporting by some FI sub-sectors appears low, including higher-risk sectors such as non-financial banking companies, the Department of Posts (MTSS services), and also rural banks. DNFBPs including higher risk sectors (e.g., corporate gatekeepers such as accountants and company secretaries as well as real estate agents) are yet to detect suspicious transactions and file STRs in a significant way. Given the risks associated with these sectors, these shortcomings were weighted heavily.

India is rated as having a moderate level of effectiveness for IO.4.

# Chapter 6. SUPERVISION

## Key Findings and Recommended Actions

### Key Findings

a) All regulated activities under the FATF Standards are subject to AML/CFT supervision in India, albeit that being new for most DNFPBs and the VASP sectors. The range and quality of supervision varies considerably among the supervisors, which range from public institutions to some newly appointed self-regulatory bodies (SRBs), with various levels of ML/TF understanding and readiness for carrying out AML/CFT supervisory responsibilities.

b) Most supervisors are broadly able to prevent criminals from controlling supervised entities and some have also implemented controls to identify unauthorised activities. However, there are insufficient checks to identify criminals and their associates in the DPMS sector, despite the application of a combination of regulatory regimes. For smaller FIs, checks do not cover shareholders with a significant controlling interest and beneficial owners. Moreover, for smaller FIs, VASPs and some DNFBPs, checks may not be sufficient to spot criminal association.

c) FI supervisors generally have a good understanding of inherent ML risks faced by the sectors they supervise, and a reasonable understanding of TF risks. There is a stronger understanding of the risks faced by the banking sector and less nuanced understanding for other financial institutions (OFIs), the securities sector, the international financial centre and rural banks.

d) Despite the recency of VASPs being covered by the AML/CFT framework, FIU-IND was able to demonstrate that it is progressing towards maintaining a well-defined understanding of risks associated with the sector. Whilst FIU-IND adopts a risk-based approach to supervision, supervisory capacity appears limited considering the complexity and growing nature of the sector.

e) DNFBP supervisors demonstrated variance in ML/TF risk understanding. CBIC (for real estate agents) and casino supervisors demonstrated a relatively good understanding while professional institutes which were recently designated as AML/CFT supervisors demonstrated a low level of understanding. The DPMS sector, as other businesses, is prohibited under tax from receiving cash of an amount over EUR 2 222, which is below the FATF-prescribed threshold. As a result, the sector fall outside the scope of preventive measures. However, there are some enforcement action

challenges, raising doubts as to whether the ML/TF risks in the sector are sufficiently mitigated by the cash restriction.

f) The main FI supervisor, the Reserve Bank of India (RBI), has an established AML/CFT supervisory model for commercial banks and larger OFIs (larger non-banking financial companies and urban co-operative banks) and has recently began conducting specific AML/CFT risk-based supervision. However, the frequency and depth of supervisory activities for the remaining OFIs is mainly driven by the entity's annual turnover, even if AML/CFT concerns are occasionally considered. The supervision of the MTSS sector, a type of MVTS identified in the NRA as posing TF risks, is not sufficiently calibrated to the risks of the sector.

g) All FI supervisors have processes in place to follow-up on shortcomings identified. A range of remedial actions are available, and there is occasional use of business restrictions (e.g., prohibition to onboard new customers) to sanction severe AML/CFT deficiencies. Whilst financial sanctions are available and have been applied for AML/CFT failures, their use was limited in number and value and not sufficiently dissuasive.

h) For the DNFBP sectors, risk-based supervision is in its early stages (except for casinos) and is characterised by limited or no capacity to supervise and monitor compliance with the obligations by the sectors including high-risk sectors. As a result, there has been very limited enforcement action which was been limited to two sectors, the casino and real estate sector.

i) Most FI supervisors demonstrated that their interventions were having a positive impact on compliance in their respective sectors. In the VASP and DNFBP sectors, due to the recency of most supervisory frameworks, there has been no or minimal impact of supervisory actions on compliance so far.

j) Supervisors and FIU-IND have issued guidance and conducted coordinated awareness-raising activities across different sectors (except for lawyers), helping to promote the understanding of ML/TF risks and AML/CFT obligations amongst regulated entities. More is required in some sectors (e.g., rural banks, accountants and TCSPs).

## Recommended Actions

### All sectors

a) Supervisors should enhance measures to ensure that fit and proper tests or other measures are consistently effective in ensuring that criminals and their associates are prevented from holding or being a beneficial owner of a significant or controlling interest, or holding a management function in all FIs/ VASPs/ DNFBPs. These measures could include, but not be limited to, wider use of criminal background checks and verification of source of wealth/funds information, in particular in higher risk sectors.

### FIs:

a) RBI should enhance its ML risk understanding of non-banking sectors and TF risk understanding across all sectors. SEBI should enhance its understanding of the ML/TF risks faced by its supervised entities.

b) RBI and SEBI should ensure that their AML/CFT supervisory action in relation to OFIs and the securities sector, respectively, is performed on an ML/TF risk sensitive basis.

c) RBI should work with MTSS principals and MTSS agents to increase the level of understanding of ML/TF risks and AML/CFT obligations by agents and subagents.

d) IFSCA, NABARD and DoP should continue to develop their ML/TF risk understanding and supervisory capacity through training and engagement with other supervisors such as the RBI.

e) All FI supervisors should ensure that the full range of sanctions are used by FIs supervisors are proportionate and dissuasive, consistent with the seriousness and impact of the specific failures.

### VASPs:

a) India should increase resources (technical and human) and capacity (including through sector-specific training) to enable the FIU-IND to adequately enhance supervision and monitoring of VASPs on a risk-sensitive basis.

b) FIU-IND should conduct sectoral and/or thematic reviews on VAs and different VASP activities to update its risk understanding.

### DNFPBs:

a) India should strengthen measures to prevent criminals or their associates from participating in the DPMS sector. Furthermore, India should enhance the monitoring and enforcement of the cash threshold prohibition in the sector.

b) India should proactively identify and commence risk-based AML/CFT supervision of distinct TCSP professionals and lawyers (i.e., TCSPs that are not company secretaries or other types of FIs/DNFBPs already subject to supervision).

c) SRBs for accountants, lawyers and company secretaries should improve the granularity of their respective ML/TF risk understanding and apply risk-based supervisory, monitoring and enforcement actions proportionate to the risks identified.

d) All DNFBP supervisors should build adequate capacity to supervise and enforce compliance.

499. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

6

## Immediate Outcome 3 (Supervision)

500. Taking into account risk, context and materiality, positive and negative aspects of supervision were weighted **most significantly** for banks; **significantly** for other financial institutions (OFIs) including MVTS, VASPs, real estate agents (REAs), TCSPs (including company secretaries) and accountants; **moderately** for the securities sector; and to **a limited extent** for casinos, lawyers, the insurance and pension sectors. See section 1.4.3 for more detail about the risk, materiality and weighting of each sector in India's context, and section 1.4.6 for a description of India's supervision arrangements.

501. FATF-defined FI, VASP and DNFBP activities are subject to AML/CFT requirements in India. Some sectors have been more recently subject to obligations: real estate agents (REAs) in 2020 and VASPs, accountants, lawyers, company secretaries and TCSPs in 2023. India designated persons providing TCSP services, who were not covered by another designation (e.g., company secretaries), as AML/CFT reporting entities in May 2023. This led to the registration of 36 TCSPs in August 2023 with FIU-IND, which is the assigned AML/CFT supervisor for this sector. In India, most company services are provided by company secretaries and accountants, whilst trust services are commonly provided by FIs in the securities sector.

502. Notaries do not perform any of the FATF-defined DNFBP activities and advocates as lawyers carry out very limited activity (e.g., preparatory work for company formation and real estate transactions). There are no other types of legal professionals in India since only advocates can practice law.

503. DPMS are not licensed or registered as a profession in India. The country subjects DPMS to tax registration and other requirements for market entry, monitoring and enforcement actions (see section 6.2.1 below). Similar to other businesses in India, DPMS are prohibited from receiving cash of an amount of INR 200 000 (EUR 2 222) or more[110], which is substantially less than the FATF-prescribed EUR 15 000.

504. Regulation and supervision of the most important FI sectors is conducted by the RBI. It is a well-established regulator and supervisor, with access to significant human resources. FIU-IND has been newly appointed to supervise the VASP sector. It also supports other regulators and supervisors across sectors identifying red flag indicators and conducting remedial actions. DNFBP supervisors range from the public sector supervisors (CBIC for real estate) to professional institutes (accountants and company secretaries). These supervisors in newly introduced sectors have less institutional experience than AML/CFT supervisors. As noted in Chapter 1, India is traditionally a 'closed' economy that has been liberalising over the last 30 years. The assessors therefore identified

[110] Income Tax Act, s.269ST.

a more hands-on approach amongst supervisors, in particular the RBI, where they were in frequent contact with the banking sector.

505. The conclusions in IO.3 are based on statistics and examples of supervisory actions provided by India; guidance issued by supervisors; interviews with supervisors and FI, DNFBP and VASP sector representatives and review of publicly available and confidential reports on the effectiveness of AML/CFT supervision in India.

### *Licensing, registration and controls preventing criminals and associates from entering the market*

506. Licensing, registration and fitness and probity checks to prevent criminals from entering the financial, VASP and DNFBP sectors are broadly adequate, but less so for some FIs in the foreign exchange and the DPMS sectors. Also, there are insufficient checks to identify criminal associates in many sectors. LEAs and some supervisors (RBI, SEBI) have dedicated resources to detect unlicensed and unregistered activity.

#### *RBI (Banks, OFIs)*

507. The RBI has comprehensive processes for licencing banks, non-banking financial companies (NBFCs) and Payment System Operators (PSOs, which provide domestic MVTS, digital payment services). These are the most material entities in terms of assets and transactions in India's financial sector.

508. *Banks:* Procedures include a multi-layer approval process within RBI; checks on fit and proper status of applicants, review of proposed corporate structure and exchange of information with other domestic and foreign regulators where needed. All persons applying to hold at least 5% of shares or voting rights in a banking company, or to be a director are required to provide extensive information in a self-declaration form, including on on-going and past investigations and convictions. Shareholders are required to provide information on source of funds and a list of relatives that are also proposed to hold shares or voting rights in the bank; directors provide information on previous experience and professional qualifications as well. The RBI checks the information against several databases and with LEAs. LEAs may also provide input in relation to suspected criminal associates. Guidelines are not explicit on checks on beneficial owners, but the RBI does not approve complex multi-layered structures for banks, unless it feels comfortable that the proposed structure does not obscure beneficial ownership identification. During the review period, there has been instances of rejection of applicants due to fit and proper concerns (see Table 6.1 below). In addition, concerns with the fit and proper' status of the promoter / promoter group, the corporate structure and/or shareholding pattern in respect of the proposed bank have led to RBI raising concerns and the applicants amending the proposed ownership and control structure.

509. *Non-Banking Financial Companies:* RBI performs checks on directors and persons applying to hold 26% of shares or voting rights of NBFCs. The RBI checks the information received against several databases and with LEAs. Similarly to the process to banks, the RBI reviews the corporate structure and has rejected or required changes to application. In at least one occasion during the review period, the RBI expressed concerns in relation to the proposed ownership structure, resulting in the NBFC's promoters proposing a change.

510. *Payment System Operators:* Even if the legal and regulatory framework is less clear (see Recommendation 26), RBI review fit and propriety of persons applying to be shareholders, directors and significant beneficial owners of PSOs performing similar checks to those done for NBFCs and banks.

511. *Foreign exchange:* For full-fledged money changers (FFMCs) and authorised dealers in foreign exchange (AD Cat II), fit and proper controls apply to directors and the entity itself. There

are no particular controls on owners and beneficial owners. The process is generally less stringent in comparison with other FIs and mainly relies on self-declarations or checks conducted by FIs themselves, although RBI may also conduct other checks. There have been cases where, due to input from LEAs, licenses were rejected due to fit and proper concerns in relation to applicant shareholders because of their connection with directors and owners of an entity whose license had been revoked due to violations in foreign exchange laws, or because of false information provided (see Box 6.1 below for an example).



### Box 6.1. Revocation of FFMC licence due to Criminal Background of FFMC Director

After renewing the license of a FFMC, the RBI learned from LEAs that one of the FFMC directors had been arrested by police in context of an investigation of an organised crime network engaged in extortion, and the laundering of proceeds of crime through foreign exchange transactions, hawala and angadia,[111] under the Gujarat Control of Terrorism and Organised Crime Act, 2015.

Whilst the arrest took place before the licence renewal, this had not been disclosed by the FFMC, as required by the regulations.

In view of the irregularities observed, the RBI issued a notice to the FFMC calling upon it to show cause as to why the process of revocation of licence under sub-section (3) of Section 10 of FEMA should not be initiated against it. The response from the FFMC was unsatisfactory and the RBI revoked the FFMC authorisation to carry out money changing business.

Source: RBI.

512. Table 6.1 below summarises the applications received during the review period and their status (approved, rejected or including rejections for "fit and proper" concerns. The main reasons for rejection were adverse feedback received from internal supervisory departments or external regulators; failure to disclose court cases or investigations in the applications; and regulatory violations by group companies.

[111] The Angadia system is a centuries-old parallel system in India where traders send cash or valuable good generally from one state to another through a person called Angadia that stands for courier. Currently, it is by and large used in the jewellery business with Mumbai – Surat being the most popular route as they are two ends of the diamond trade. Angadians generally specialise in the secure transportation of valuable goods, including precious metals and stones. It originated in the state of Gujarat.

### Table 6.1. Application for new licences

| No. of Applications | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| **Universal Banks and Small Finance Banks** | | | | | |
| Received | 2 | 2 | 5 | 3 | 1 |
| Approved | 1 | - | 1 | - | - |
| Rejected | 1 | 2 | 2 | - | - |
| In process | - | - | 2 | 3 | 1 |
| **Non-Banking Financial Companies** | | | | | |
| Received | 408 | 416 | 247 | 276 | 211 |
| Approved | 132 | 94 | 55 | 55 | 33 |
| Returned | 212 | 250 | 154 | 190 | 161 |
| Rejected | 64 | 72 | 38 | 31 | 17 |
| **Full-fledged Money Changers** | | | | | |
| Received | 147 | 255 | 84 | 132 | 296 |
| Approved | 136 | 190 | 55 | 61 | 131 |
| Returned or Rejected | 11 | 65 | 29 | 71 | 158 |
| In process | | | | | 7 |
| **Authorised dealers in foreign exchange** | | | | | |
| Received | 0 | 2 | 0 | 1 | 7 |
| Approved | 0 | 1 | 0 | 0 | 1 |
| Returned ((for applicant to address an issue) | 0 | 1 | 0 | 0 | 4 |
| Rejected | 0 | 1 | 0 | 0 | 2 |
| **Payment System Operators** | | | | | |
| Received | 6 | 29 | 34 | 152 | 66 |
| Approved | 0 | 6 | 0 | 0 | 1 |
| In-principle approval | 0 | 0 | 6 | 51 | 17 |
| Under process | 0 | 0 | 0 | 2 | 17 |
| Rejected / Returned | 6 | 23 | 28 | 99 | 31 |
| **Indian Agents – Money Transfer Service Scheme** | | | | | |
| Received | N/A | N/A | 5 | 4 | 0 |
| Approved | N/A | N/A | 5 | 4 | 0 |
| Returned/Rejected | N/A | N/A | 0 | 0 | 0 |

Source: RBI

513. After licensing or authorisation is granted to a bank, the acquisition of more than 5% of equity shares as well as the appointment of senior management also requires RBI approval. For NBFCs, RBI approves acquisitions of 26% or more equity shares in NBFCs, since financial year 2021-2022. Among the reasons for rejection of new shareholders there were concerns that the applicants were from FATF-listed jurisdictions or because the source of funds was not substantiated. For the foreign exchange sector, there are checks for changes in senior management but not for change in ownership. Acquisition or change in control of PSOs, if by an entity not previously authorised by RBI for undertaking similar activity, also needs RBI's prior approval.

### Table 6.2. Applications for acquisitions of equity shares in Banks and NBFCs

| No. of Applications | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| **Universal Banks and Small Finance Banks** | | | | | |
| Received | 4 | 1 | 11 | 5 | 17 |
| Approved | 4 | 1 | 7 | 5 | 14 |
| Rejected | - | - | 4 | - | 3 |
| **Non-Banking Financial Companies** | | | | | |
| Received | N/A | N/A | N/A | 39 | 40 |
| Approved | N/A | N/A | N/A | 31 | 22 |
| Rejected | N/A | N/A | N/A | 8 | 18 |

Source: RBI

### Table 6.3. Applications for appointment/re-appointment of personnel at senior level in private sector banks

| No. of Applications | 2018-19 | | 2019-20 | | 2020-21 | | 2021-22 | | 2022-23 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | P | R | P | R | P | R | P | R | P | R |
| CEO / Managing Director | 25 | 8 | 44 | - | 56 | 1 | 65 | 2 | 40 | - |
| Non-Executive Director | 1 | 1 | - | - | 1 | - | 1 | - | | |
| Part time Chairman | 12 | 0 | 10 | - | 18 | 2 | 24 | 4 | 19 | 4 |
| Whole Time Director/ Executive Director | 4 | 0 | 16 | 4 | 6 | - | 4 | - | 15 | - |
| Others | - | - | - | - | 2 | - | 9 | - | | |

Note: P – Processed, R- Rejected.
Source: RBI

514. To identify unauthorised FIs, the RBI has established a Market Intelligence Cell within Department of Supervision and also relies on intelligence shared by regulated entities or other authorities. The RBI publishes a list of authorised entities in its website and there is a portal where any citizen can file a complaint about unauthorised FIs.[112] India also relies on the work of LEAs to disrupt hawala and other informal networks, which present risks for ML and TF (see chapter 1). Where illegal remittances are noticed as part of investigation of other crimes, LEAs also investigate the remittance aspects. For instance, the ED has dedicated units that collect intelligence, including on hawala, and can also receive anonymous complaints. The ED and other LEAs have a strong focus on the investigation of hawala networks where remittances are used to launder money or to finance terrorism activities or where organised criminal organisations are involved. This is evidenced by a varied of case studies of successful investigation and prosecution of hawaladars operating in India included in the analysis of Immediate Outcomes 7 and 9.

*Other FI supervisors (SEBI, IFSCA, IRDAI, PRFDA)*[113]

515. *Securities, insurance and pensions*: SEBI, IRDAI and PRFDA apply fit and proper tests on persons proposing to own, control, directly or indirectly, or hold a senior management position of a securities insurance and pension firm respectively, as well as their beneficial owners. Regulators

[112] https://sachet.rbi.org.in/home/index

[113] DoP and NABARD do not perform licensing activities. All post offices, including postal banks/MVTS, are directly owned by the government of India. For rural banks supervised by NABARD, RBI is responsible for licensing procedures.

request self-declaration on criminal convictions and check applicants against databases of criminal records, on an ad hoc basis. Supervisors maintain statistics on applications, approvals and rejections. Rejections included cases of 'fit and proper' concerns for securities firms (SEBI) and insurance firms (IRDAI). License renewals provide for an opportunity to reapply checks. There are no specific checks to identify criminal associates.

516. SEBI's supervised entities are diverse, from stock exchanges with very large balance sheets, to smaller portfolio managers and investment advisers, and licencing and fit and proper procedures vary. For intermediaries (e.g., stockbrokers, depository participants and investment advisors), SEBI relies on stock exchanges and other market infrastructure institutions (MIIs) to perform initial checks. SEBI performs checks in some applications and may seek information from other regulators where the applicant is also regulated by them, performing checks against its databases. These additional checks have led to rejections (i.e., in year 2022-23, five applications for stockbroker/depository participant were returned). Concerning unlicensed activities, SEBI promotes awareness campaigns about the risk posed by unlicensed brokers and dealers and takes action on the basis of complaints. The main challenge SEBI has identified relates to unregistered investment advisors, as their activities are less visible in the securities market. Stock exchanges also have systems in place to identify unlicensed players, e.g., by undertaking "mystery shopper" exercises and screening internet and social media. Statistics on applications and cancellations are included in the table below:



### Table 6.4. Details of registration granted and cancelled in respect of securities intermediaries.

| No. of Applications | 2018-19 | | 2019-20 | | 2020-21 | | 2021-22 | | 2022-23 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | G | C | G | C | G | C | G | C | G | C |
| Stock Exchanges | - | - | - | - | - | - | - | - | - | 1 |
| Depositories | - | - | - | - | - | - | - | - | - | - |
| Alternative Investment Funds, Foreign Venture Capital Investors and Venture Capital Funds | 162 | 5 | 126 | 29 | 110 | 13 | 172 | 7 | 237 | 48 |
| Bankers to an Issue, Credit Rating Agencies, Debenture Trustees and KYC Registration Agencies | 2 | - | 2 | - | 3 | 0 | 1 | 4 | 3 | 11 |
| Custodians | 1 | 3 | 1 | - | 1 | 1 | - | - | - | 2 |
| Depository Participants | 20 | 27 | 28 | 24 | 29 | 43 | 35 | 42 | 36 | 26 |
| Foreign Portfolio Investors | 821 | 611 | 1138 | 866 | 840 | 372 | 1184 | 478 | 1183 | 723 |
| Infrastructure Investment Trusts & Real Estate Investment Trusts | 4 | 1 | 3 | 2 | 6 | - | 3 | - | 3 | 1 |
| Investment Advisors and Research Analysts | 309 | 25 | 177 | 22 | 182 | 60 | 208 | 115 | 358 | 346 |
| Merchant Bankers | 17 | 9 | 10 | 5 | 6 | 0 | 11 | 5 | 9 | 8 |
| Mutual Funds | 2 | 2 | 1 | 0 | 0 | 0 | 2 | 1 | 1 | 2 |
| Portfolio Managers | 45 | 63 | 41 | 17 | 20 | 10 | 23 | 17 | 53 | 19 |
| Registrars to an Issue & Share Transfer Agents | 6 | - | 5 | 2 | 1 | 1 | 6 | 5 | 2 | 5 |
| Stockbrokers | 545 | 478 | 317 | 482 | 291 | 509 | 346 | 398 | 213 | 387 |

Note: G – Registration Granted, C – Registration Cancelled, Surrendered or Suspended.
Source: SEBI

517. *International financial centre*: Since October 2020, IFSCA is responsible for performing fit and proper checks on applicants that wish to operate in the IFSC, as well their owners and controllers and key managerial personnel. IFSCA apply the same licensing framework that applies for the type of FI in the rest of India (e.g., IFSCA applies the RBI framework in connection to banks,

the SEBI framework for security firms). So far, IFSCA has rejected/returned 14 applications of FIs and 14 applications of DNFBPs. Previously, IFSC entities were directly licensed by RBI, SEBI and IRDAI. IFSCA employs some former staff from other FI regulators, who are familiar with main regulatory requirements. Most FIs operating in the IFSC are branches of Indian or foreign entities and IFSCA seeks inputs from other domestic supervisors (e.g., RBI and SEBI) concerning Indian groups and foreign groups are asked to provide a "no objection certificate" from the home regulator. So far, IFSCA has not exchanged information with foreign supervisors.

518. *Rural banks and Department of Posts:* Rural banks are licensed by the RBI and supervised by NABARD. There have been no rural bank licenses issued during the review period. In relation to financial services provided by the Indian Post, no market entry requirements apply, as all post offices are owned by the government of India and managerial personnel are public employees, hired in accordance with regular civil servant appointment rules, which include screening processes and criminal backgrounds checks.

*FIU-IND (VASPs)*

519. In March 2023, FIU-IND was designated as the AML/CFT supervisor for the VASP sector. Since then, VASPs that had already been operating in India before March 2023 (see Chapter 1) or have since commenced operations and applied for registration. FIU-IND applies market entry measures to prevent criminals and their associates from participating in the sector.[114] This includes an examination of the VASPs' corporate structure and beneficial owners; criminal background checks of directors, shareholders and partners, as well as beneficial owners, using LEA databases, and in-person meetings with applicants, including the VASP principal officer. Managers, shareholders, principal officer, designated and other directors are also screened against databases at the time or registration of the entity and during offsite supervision. Information on source of funds is not collected and could be helpful to identify criminal association.

520. As at November 2023, FIU-IND received 38 applications, resulting in 28 VASPs registered, and two rejections, one application was withdrawn, and seven were still undergoing the registration process. The rejected applications related to failure to submit tax documentation; or an entity's decision not to commence business after its application.

521. FIU-IND uses market intelligence, social media and public source scraping to identify unregistered VASPs. So far it has detected 11 unregistered VASPs which were approached for registration, seven of which are fully registered and the remaining four are undergoing registration. LEAs have also identified three unregistered VASPs, which were also approached by FIU-IND for registration.

*DNFBPs*

522. Regulators of DNFBPs generally rely on market entry controls underpinned by regulations on professional accreditation or other regulatory requirements, and have applied these processes and procedures to identify criminals or their associates seeking to owning or controlling a business in the DNFBP sector.

523. For DPMS, India applies tax and company registrations requirements, self-regulatory body membership (required for importer and exporters) and registration with the Bureau of Indian Standards for hallmarking of precious metal jewellery which together require a broad range of information from applicants for market entry. While the market entry measures for a high-risk

[114] As per FIU-IND circular No. 9-8/2023/COMPL/FIU-IND dated 17 October 2023.

segment of the sector such as export and import are largely in place, there are some challenges as requirements will not systemically apply to all DPMS, depending on their activity or setup.

### *Real Estate Agents and Professionals (Chartered Accountants, Cost Accountants, TCSPs, including Company Secretaries)*

524. *Real estate sector:* The State Real Estate Regulatory Authorities (RERAs) met during the on-site have demonstrated application of procedures for checking the fitness and probity of applicants prior to authorising activities for selling and buying of real estate in each State and on a continuous basis. The statutory framework for real estate agents for both individuals and entities is decentralised and each State RERA is responsible for market entry controls in its State. The State RERAs' procedures are harmonised together with the Inspector-General of Registration (for database of buyers and sellers in real estate transactions) ensuring verification of applicants between the States and property transactions conducted.

525. For registration, real estate agents can be individuals and legal structures which are both vetted for probity and fitness focusing on verification of identities of the agents and promoters through company and individual information, such as Permanent Account Number (PAN),[115] professional certification and details of company formation and business address of a real estate agency. The authenticity and reliability of the information, which includes checks on criminal and regulatory records, is verified through independent sources (e.g., registries and private databases) in addition to review of audited business accounts. This process has assisted the State RERAs to identify non-compliant real estate agents and establish links with unauthorised third parties.

526. *Accountants, company secretaries and other TCSPs:* The market entry measures of the self-regulatory bodies (SRBs) for accountants and company secretaries show fit and proper criteria at inception and renewal stages, and instituted enforcement actions for violations. SRBs are professional institutes at central government and control market entry of chartered accountants, cost management accountants, and company secretaries through robust checks which include professional accreditation, and compliance with regulation and codes of ethics. Individuals applying for accreditation provide self-declaration (including information on convictions) and a certificate of fitness and appropriateness signed by two members of the profession. The professional institutes identified market entry violations and applied enforcement measures such as suspensions and terminations.

527. There are no market entry requirements for TCSPs that are not covered by other requirements (e.g., being an FI or company secretary for instance). Since August 2023, these TCSPs are subject to registration with the FIU-IND. In order to register, they need to provide information on their corporate structure including details of significant beneficial owners as well as self-declarations stating that there are no criminal proceedings initiated or pending against directors/ partners. It is unclear what checks are performed for owners including beneficial owners of a TCSP firm or which checks would identify criminal association.

### *Other DNBFPs (Lawyers, Casinos and DPMS)*

528. *Lawyers (including notaries):* State Bar Councils are responsible for regulation of the profession and have applied market entry procedures though checks for professional accreditation, regulatory and criminal records in addition to regular and ad-hoc reviews for annual memberships approvals. Sanctions for compliance failures such as suspensions and terminations have been applied during the period under review.

[115] A ten-digit alphanumerical number issued by the Income Tax Department.

529. *Casinos:* The policy decision for regulation of casino operations lies in each State. Market entry checks conducted by the regulators in the States of Sikkim and Goa,[116] cover bank statements and audited financial statements for financial soundness, voting rights and shareholders to determine eligibility of owners including BOs and related parties, key management persons and criminal or regulatory records at authorisation and lifecycle of a casino. Examples of contravention of casino regulatory rules were identified and proportionate and dissuasive enforcement action were applied.

530. *DPMS:* India prohibits businesses, including DPMS, from engaging in cash transactions above INR 200 000 (EUR 2 222) which is substantially below the FATF designated threshold for AML/CFT purposes. In practice, India relies on existing market entry requirements for DPMS, monitored and enforced by different public and private sector. The sector is subject to an interlinked system comprising (a) tax registration – DPMS businesses carrying out transactions above INR 200 000 must comply with tax obligations, (b) company incorporation – DPMS that incorporate as companies or LLPs must comply with incorporation regulations, (c) hallmarking legal requirements – hallmarking on precious metal jewellery is compulsory in India since April 2023. Only DPMS registered with Bureau of Indian Standard (BIS) can perform hallmarking and sell hallmarked jewellery; (d) DPMS involved in import and export of gold and diamonds are required to register with Gems and Jewellery Export Promotion Council (GJEPC). The certificates of GJEPC membership and General Sales Tax (GST) registration are mandatory for import/export of gems. GJEPC has over 9 500 members, which refers to less than 8% of the DPMS businesses in India that are registered with BIS as GJEPC membership only required for businesses that import and export of gold and diamonds.

531. While the tax and incorporation registries follow prescribed approval processes, the regional GJEPC procedures rely on the 'MyKYC' platform (a global online KYC repository for gems and jewellery) and a dedicated KYC Team for vetting GJEPC applicants (normally DPMS involved in import and export), which includes virtual and location-based meetings in each region prior to granting authorisation.

532. For a DPMS company engaged in import and export and production or sale of hallmarked jewellery, the regimes above altogether obtain and verify proof of identity, residential and business address, bank account, TFS and PEPs screenings, incorporation documents and criminal and regulatory checks. During the period under review, there were 84 removals and 44 renewal rejections of applications by GJEPC due to unreliable proof of identity and business address and other fit and proper failures. In addition, there were 224 sanctions against DPMS for GST violations.

533. Actions by the GJEPC appear effective since the DPMS involved in import and export will not be able to do so without the mandatory membership certificate. However, although GJEPC has over 9 500 members, and there are approximately 175 000 DPMS businesses in India.

### *Supervisors' understanding and identification of ML/TF risks*

534. FI supervisors generally have a good or reasonable understanding of inherent ML risks faced by the sectors they supervise, and some understanding of TF risks. FI supervisors contributed to the 2022 NRA and participate in several coordination platforms in maintaining their risk understanding up to date. Sector-specific ML/TF risk understanding is more developed in relation to commercial banks and larger NBFCs/UCBs and less developed in relation to OFIs.

[116] Casinos have only been permitted to operate in Goa and Sikkim. See Chapter 1.

535. The risk understanding of the VASP supervisor (FIU-IND) is reasonable, especially considering the recency of its supervisory activities, but the SRA needs to be updated. In the DNFBP sector, supervisors' ML/TF risk understanding is generally in its early stages.

*RBI (Banks, OFIs)*

536. The RBI has a very good understanding of the ML risks faced by the banking sector. Understanding of TF risk is reasonable, but less developed when compared with ML risk understanding. The RBI has undertaken two SRAs focused on ML risks during the review period, in 2019 and 2022 and strongly contributed to the NRA process. The SRA exercises involved the sampling of 10 banks, covering different types of banks such as public, private, foreign, UCBs) and the analysis of 20 of their products across 13 parameters. Products included private banking accounts; current accounts of proprietors/partners, legal persons, trusts; trade finance products; foreign exchange remittances, pre-paid cards, custodial services, walk-in customers, third-party products. Parameters included: total value, average transaction size, client base profile, level of cash activity, frequency of international transactions, vulnerability factors (e.g., existence of ML typologies on the abuse of the product/service, use of the product/service in fraud or tax evasion schemes, non-face-to-face use of the product/service, delivery of the product/service through agents).

537. Whilst no specific TF SRA was conducted, TF risk features that are common to ML were captured in the two SRAs. RBI's risk understanding is further substantiated by its close engagement with supervised entities, the FIU-IND, LEAs, and other supervisors. This includes regular meetings with FIs on ML typologies, modus-operandi of frauds, ML/TF risk perception and mitigating measures; quarterly meetings of nodal officers of financial sector regulators and FIU-IND; and information sharing with LEAs and FIU-IND.

538. In 2020, the RBI developed a data-intensive analytical model which allows it to understand a bank's vulnerabilities associated with ML and TF. Approximately 90 banks submit, on a quarterly basis, a comprehensive data template with over 750 data points, covering topics such as policy on frequency to update CDD; transaction monitoring systems; products, services and delivery channels; risk profile of face-to-face and non-face-to-face customers; profile of respondent/correspondent banks; risk profile of new customers; jurisdictions in or with which bank, bank's group entities have presence and/or operations; transaction profile of walk-in customers; number of existing customers where periodic updating/ on-going due-diligence is pending; identification of money mules; details on cross border transactions; alert management (e.g. time to analyse alerts); details of cash transactions; details of small accounts; number of customers on sanctions lists and amounts of assets frozen.

539. Based on the data submitted, RBI develops approximately 450 risk indicators as well as risk scores for each entity on an annual basis. The risk scores and risk profiles are updated annually, when emerging risks are also taken into account (e.g., data points and risk indicators on identification of money mules were added to the RBI model later, following its findings on cyber enabled frauds). A customised version of the analytical model has been used since 2022 to collect information of the larger NBFCs and larger UCBs and develop specific risk profiles for that sector.

540. Some of the main ML/TF vulnerabilities identified using the SRA and the analytical model were frauds and in particular cyber frauds, AML/CFT knowledge of bank staff, availability of beneficial ownership information and quality of customer due diligence. In terms of products, risks were identified in relation to mule accounts (in particular in non-face-to-face onboarding), accounts held by sole proprietorships and partnerships (linked to a number of fraud cases), foreign exchange remittances and retail savings accounts in private banking (a frequently used banking product, where several typologies were identified; e.g., high cash deposit, money mule accounts used for smurfing).

541. The understanding of ML/TF risks at sectoral level across all the sectors it supervised is generally good. RBI SRAs covered, in addition to banks, a range of FIs (NBFCs, UCBs, MTSS operators, FFMCs, PPI issuers, PSOs). Risk mitigation measures have been assessed in relation to each sub-sector as part of the calculation of residual risk. Understanding of ML/TF risks at institutional level is more developed for commercial banks and larger NBFCs/UCBs.

542. RBI's SRAs did not cover TF risks directly, but considered several features that are common to ML and TF. The analytical models also capture some data points pertaining to TF vulnerabilities such as the "amount of cross-border flow of funds from and to different categories of jurisdictions" and "data on freezing of assets under section 51A of UAPA". In addition, onsite inspection covers examination of TFS related processes and systems. RBI's TF risk understanding appears, nonetheless, to be less developed or granular than understanding of ML risk.

*Other FI supervisors (SEBI, IFSCA, IRDAI, PFRDA, NABARD and DoP)*

543. All of the other main FI supervisors continue to build their ML/TF understanding on the basis of their supervisory findings as well as regular meetings with FIU-IND and other supervisors. The level of ML/TF risk understanding varies between supervisors.

544. *Securities:* In addition to the NRA, SEBI builds its risk understanding on other risk assessment exercises conducted in the past, covering issues such as CDD, audit and governance, transaction monitoring and staff training. The NRA assessed the ML threat in the securities sector as medium, considering the number of insider trading and market manipulation cases that have led to ML investigations, and vulnerability as medium low. SEBI considers securities fraud as well as mutual funds, due to their broad client base, including higher risk clients, as posing higher threats and vulnerabilities. SEBI is largely reliant on in-built controls of the sector – i.e., transactions conducted via banks, prohibition on cash transactions, need for tax registration number (PAN) to assess the ML/TF risk of the sector. Those controls were developed based on SEBI's understanding of risks associated with the securities market. Whilst this is acknowledged, SEBI did not demonstrate a more nuanced understanding of how the securities sector in general or products offered by the sector have or can be misused for ML or TF or an understanding of residual risks in the sector. SEBI also uses a surveillance mechanism to monitor activities across market segments – such as unfair trading practices, market manipulation, front running, and insider trading - which are ML predicate offences.

545. *International financial centre:* IFSCA conducted an SRA in July 2023, where the residual ML/TF risks of the fintech sector were assessed as medium, and the risks of the banking and most of other sectors were assessed as medium-low. The SRA does not clearly identify specific ML or TF threats in the IFSC, but IFSCA was able to elaborate on those to some extent, in particular risks associated with TBML and export financing, during the on-site visit. Despite IFSCA's participation in the process, the NRA does not make explicit reference to ML/TF risks of the IFSC and the extent to which they would differ from the ones of the rest of India.

546. *Department of Posts:* The DoP demonstrated that it understands the ML risks of its sector to some extent. It has undertaken an SRA for the different financial products it offers, most of which were considered low risk for ML and TF, mainly due to the low amounts of deposits and transfers permitted. However, DOP demonstrated a more limited understanding of TF risks during the onsite, focusing exclusively on TFS obligations, although it operates as an agent for an important MTSS.

547. *Rural banks:* NABARD is yet to develop an understanding of ML/TF risks associated with the rural banking sector. It considers the ML/TF risks in the sector to be low on the basis that supervised entities mainly provide financial services to farmers, artisans or other small business in rural areas.

548. *Insurance and pensions:* IRDAI has developed a good sectorial understanding of risks in the insurance sector, including how different characteristics of insurance products and services influence their exposure to ML/TF risks. It can benefit from a more granular ML/TF risk profile of its supervised entities, PFRDA has a reasonable understanding of ML/TF risks and the mitigation measures in place that limits the sector's exposure to ML/TF risks (e.g., long vesting period, no cash transaction, payments from the banking system).

*FIU-IND (VASPs)*

549. FIU-IND is developing its understanding of the ML and TF risks of the VASP sector in a positive manner despite the recency of its supervisory function. Risk understanding is being informed by its engagement with LEAs in monthly meetings of the virtual assets contact group, with VASPs and other FIs in the sub-working group on peer-to-peer transactions and cybercrimes, as well as by its supervisory activities.

550. Just before VASPs were brought to the AML/CFT framework in March 2023, the Department of Revenue conducted an SRA of the sector. The SRA did not include qualitative and quantitative information from the domestic and international market and the considerations on AML/CFT risks on the SRA were vague due to limited insights into the sector. In addition, considering the fast-paced developments in the sector following the conclusion of the SRA, including India's market entry requirements for the sector, preventative measures beginning to be applied and tax requirements being imposed on transactions, the SRA does not currently reflect the VASP landscape in India. India's plan is to review the SRA on an annual basis, which seems adequate considering the changing landscape of the sector.

*DNFBPs*

551. ML/TF risk understanding in the DNFBP sector is evolving and varied by supervisor. Supervisors of casinos and real estate agents demonstrated better risk understanding at sectoral and institutional levels than supervisors of professionals**.**

552. *Real Estate Agents:* CBIC, the AML/CFT supervisor for real estate agents, has a good ML/TF risk understanding at sectoral level (based on NRA results) and to a lesser extent at institutional levels. The revenue risk assessment of the CBIC covers 34 audit risk parameters as opposed to a few broad risk factors for ML/TF risk assessment. In general, the supervisor relies on information about (a) high-risk jurisdictions and countries in FATF increased monitoring process, (b) enforcement actions taken against entity and (c) frequency of transactions reported.

553. For the real estate agents, the CBIC has a good appreciation of the risks related to *benami (nominee)* and cash transactions and high value transactions in the eight urban market (80 % of the transaction values) of 28 States. The CBIC's ML/TF risk understanding seems aligned with the central government measures of promoting transparency of real estate transactions through prohibition of cash and *benami* transactions, which have reduced ML/TF risks and promoted tax compliance in the sector.

554. *Professionals:* The supervisors of the professionals demonstrated an evolving ML/TF risk understanding relying on the results of the NRA and the separate risk assessment of legal persons and arrangements which do not provide granular details for informing proportionate supervisory actions. This situation is likely to improve following the designation in May 2023 of SRBs as AML/CFT supervisors which was a few months before the onsite visit.

555. *Casinos:* Casino supervisors have risk assessment tools with relevant risk information (i.e., weekly bilateral meetings, NRA results, quarterly entity returns and surveillance) which has led to the supervisors having a reasonable understanding of ML/TF risks at sectoral and entity levels, in particular risks associated with cash, with significant mitigating measures limiting risks

(prohibition of cash purchases of chips/token above INR 50 000 (EUR 562) and a 30 percent tax deduction on every INR 10 000 (EUR 112) won).

### *Risk-based supervision of compliance with AML/CFT requirements*

556. There is an uneven sophistication and maturity levels of risk-based application of supervision. In the financial sector, the frequency and depth of the supervision of commercial banks and larger UCBs & NBFCs has been informed by ML/TF risk to an increasing degree. In many sectors, however, supervisory attention is still mainly based on size of entity and turnover, although aspects of ML/TF risks are taken into consideration to varying degrees. FIU-IND has commenced risk-based supervision of VASPs. In the DNFBP sector, a few supervisors have in place supervisory measures while most are building capacity to commence supervisory actions.



*RBI (Banks, OFIs)*

557. The RBI supervises commercial banks, UCBs and NBFCs based on a continuous engagement with these firms, with 720 staff supporting this activity. Prudential and AML/CFT teams cooperate and co-ordinate well and have a common management structure. This involves on-going offsite engagement, with quarterly reports by this group of FIs and annual feedback by RBI. The commercial bank sector receives the utmost supervisory attention because most transactions (domestic and cross border) are routed through the banking system.

558. Most commercial banks as well as larger NBFCs and UCBs are subject to annual on-site inspections, which are focused on prudential aspects but also cover AML/CFT elements. These elements are defined on the basis of priority topics identified by RBI for each supervisory cycle and/or entity specific issues.

559. Moreover, in 2020, the RBI created a 'KYC-AML group' in the Department of Supervision, which is fully dedicated to AML/CFT supervision. The 'KYC-AML group has first focused on the oversight of commercial banks and, since 2022, on larger NBFCs and UCBs. It conducts regular off-site monitoring and has started performing on-site inspections. As part of off-site monitoring, all commercial banks submit approximately 750 data points related to AML/CFT, to the RBI on a quarterly basis (see 6.2.2 above). These data points are inputted into a risk matrix and used to determine each bank's risk score and overall risk profile, weighted according to a methodology. The risk matrix also allows the determination of areas where a bank is an outlier in comparison with other banks (e.g., a bank that reports a very small or very large proportion of clients classified as high-risk). Such information is shared with the bank and further analysed during prudential and AML/CFT focused on-site inspections.

560. The RBI has conducted AML-CFT dedicated on-site inspections for the five banks classified as high risk and two banks classified as medium risk in 2021-22 (some of them have been inspected more than once). On-site inspections are targeted at higher-risk banks and other higher-risk NBFCs and UCBs, based on their off-site risk assessments, materiality, turnover, internal / external inputs, requests from prudential supervisory teams and results of previous assessments. Where possible, these on-sites take place in coordination with the prudential supervision team. A summary of prudential and AML focused on-sites is included in the table below:

**Table 6.5. On-site inspections for prudential supervisory assessment and AML/CFT focused assessment of banks by RBI**

| Financial Year | No. of banks covered | |
|---|---|---|
| | Prudential supervision, also covering AML/CFT elements | Focused KYC/AML supervision |
| 2019-20 | 104 | - |
| 2020-21 | 81 | 3 |
| 2021-22 | 41[117] | 7 |
| 2022-23 | 60 | 6 |

Source: RBI

561. Since 2022, the RBI also performs thematic reviews across all or a selected group of commercial banks to assess compliance over a particular topic or to monitor implementation of specific rules. The thematic reviews performed so far on areas related to AML/CFT, such as the identification of mule bank accounts (2023) and periodic updates of CDD as well as pendency with filing information with the Central KYC Registry (2023). They have helped generate improvements in these areas, as detailed in section 6.2.5 below.

562. For NBFCs and UCBs, off-site AML/CFT specific monitoring has been implemented to the largest NBFCs and UCBs – i.e., 56 NBFCs, corresponding to 43% of the total asset size of the sector; and 41 UCBs, corresponding to 43% of the total of the sector. These entities submit over 400 data points to RBI on a quarterly basis to analyse and follow-up upon accordingly. This includes risk rating the covered NBFCs and UCBs. On-site inspections have been completed for the three higher risk UCBs identified in the financial year of 2021-2022. The RBI has also started to develop risk profiling of NBFCs, based on size and activity (e.g., deposit taking). Off-site findings including areas of concern for NBFCs and UCBs are shared in writing and entities are advised to take appropriate action.

563. The inspection cycle of remaining OFIs (FFMCs, MTSS and authorised foreign exchange dealers) is defined mainly on the basis of turnover and volume of transactions, although in some cases the inspection periodicity has been adjusted based on supervisory concerns, including about AML/CFT compliance. These OFIs are subject to on-site inspections which cover ML/TF aspects. Snap inspections can be added to the inspection planning resulting from, for instance, supervisory concerns arising from findings (see Box 6.2 below) or feedback from LEAs.

[117] With the adoption of a 'calibrated' supervisory approach in the year 2019 and onwards, all the banks, especially the smaller banks, are not subjected to onsite inspection every year. Accordingly, the number has gone down.

### Box 6.2. Adjustment of inspection periodicity on the basis of AML/CFT concerns

RBI inspected an FFMC (which is also operates as an MTSS agent) in February 2021. The inspection revealed certain AML/CFT and other shortcomings. As per the turnover criteria, regular inspection of the FFMC was to be conducted once in 3 years. However, considering the supervisory concerns, the inspection periodicity was adjusted, and subsequent inspections were carried out in June 2022, resulting in monetary penalty and strong cautionary advice issued in May 2023.

Source: RBI.



564. For PSOs (a type of domestic MVTS), the frequency of supervisory activities is driven primarily by prudential factors, such as transaction volume and market share, although ML/TF criteria are also taken into consideration. Similarly, to the foreign exchange sector, the frequency of supervisory activities may be adjusted depending on input from LEAs or other developments (e.g., media adverse reports). For the purpose of inspections, PSOs are classified as large, medium or small.

565. Outside the banking and large NBFC/UCB sectors, no specific classification was developed on considerations of ML/TF risks relating to factors such as the nature of the specific product or service, delivery channel, customer base, geographic location, or sophistication of internal controls to inform supervision.

566. The table below illustrates the supervisory activities in the OFI sector (except MTSS, which is dealt with below):

### Table 6.6.Prudential on-site inspections, covering AML/CFT elements, on other FIs supervised by RBI

| Financial Year | Total No. of entities | No. of inspections | | |
|---|---|---|---|---|
| **Full Fledged Money Changers (FFMCs)** | | **On-site** | **Off-site** | **Snap** |
| 2018-19 | 1 770 | 650 | -- | 3 |
| 2019-20 | 1 864 | 581 | -- | 12 |
| 2020-21 | 1 986 | 263 | 184 | 5 |
| 2021-22 | 1 887 | 601 | 102 | 2 |
| 2022-23 | 1 835 | 554 | 23 | 29 |
| **Authorised dealers in foreign exchange** | | **On-site** | **Off-site** | **Snap** |
| 2018-19 | 37 | 35 | - | - |
| 2019-20 | 39 | 35 | - | - |
| 2020-21 | 41 | 21 | 7 | - |
| 2021-22 | 42 | 25 | 8 | - |
| 2022-23 | 43 | 34 | 1 | 6 |
| **Payment System Operators (PSOs)** | **Total No. of entities** | **No. of inspections** | | |
| 2018-19 | 88 | | | 42 |
| 2019-20 | 82 | | | 25 |
| 2020-21 | 78 | | | 31 |
| 2021-22 | 66 | | | 45 |
| 2022-23 | 68 | | | 44 |

Source: RBI

567. In relation to MTSS, RBI licences the overseas principals and conducts off-site surveillance and monitoring by requesting them to submit information such as an annual self-assessment, information on their fraud monitoring / alert systems. RBI occasionally meets with the overseas principals, and/or reviews market intelligence on them. Indian agents are required to be registered or licensed with the RBI and are required to be either a bank, authorised dealers (Category-I Category-II) in foreign exchange (including NBFC) or FFMC or Department of Post. In that capacity, they are subject to regular supervisory engagement with RBI that apply to each sector, as described above. The Department of Posts is also a MTSS agent (see more details below).

568. It remains for the overseas principles to monitor AML/CFT compliance with their Indian agents and subagents (i.e., money changers). Considering the NRA findings, where the MTSS sheme was identified as posing a high risk for TF across two of the six theatres,[118] the RBI conducted a snap audit of all MTSS Indian agents that are not banks/NBFCs in 2023 (covering 12 out of the total population of 22 agents), with special emphasis on the implementation of AML/CFT guidelines. The main findings of this audit were not shared with the assessment team, although RBI has shared the actions taken against some of the Indian agents, which ranged from cautionary advice to monetary penalties. Indian agents are required to conduct monthly audits and annual on-site inspections of all sub agents' locations.

*Other FI supervisors (SEBI, IFSCA, IRDAI, PFRDA, NABARD and DoP)*

569. *Securities:* SEBI uses a range of supervisory tools (off-site, on-site, thematic inspections, system audits) to monitor compliance by its supervised population and AML/CFT elements are considered as part of inspections; however, those are mainly triggered on the basis on prudential considerations rather than ML/TF risks. In 2021, there has been a thematic exercise on AML/CFT aspects covering ten entities (stockbrokers and depository participants). Topics included onboarding of new clients, alert generation on CDD process at exchanges, CDD verification process and compliance with SEBI's Master Circular on AML/CFT. Stock exchanges and Depositories also perform a supervisory role in respect of intermediaries, covering AML/CFT compliance aspects as part of general inspections. Those inspections are similarly decided on the basis of broader considerations (e.g., financial strength of intermediaries, number of clients/fund of clients, reports of internal audits).

570. *International financial centre:* Starting in 2023, IFSCA conducted AML/CFT off-site monitoring, including topics such as transaction monitoring and screening across all IFSC sectors as well as banks' operating models. On that basis, IFSCA categorised IFSC institutions according to ML/TF risk profile. On-site inspections have been completed for the banks identified as higher risk (i.e., five medium-high banks) in 2022-23 and two medium-low risk banks in the 2023-2024 cycle, prior to the on-site visit. The remaining medium-low and low risk categorised banks will be inspected in the next two years. Other sectors have not been subject to onsite inspections yet.

571. *Department of Posts:* The DoP inspects branch and subsidiary post offices every year and head post offices twice a year in connection with their provision of financial services products. Those inspections cover some general AML/CFT aspects. There is no external audit or supervision by other government authorities, and this may be desirable to ensure adequate AML/CFT controls are in place, drawing on the AML/CFT expertise of other supervisors. India's 2023 Action Plan identified specific actions to be taken by DoP to ensure compliance with AML/CFT norms and RBI master direction to MTSS in respect of international money orders. For MVTS (remittances), **DoP**

[118] After cash-couriers and hawala. See Chapter 1.

is an Indian agent and uses its post office network for a major international MVTS chain, which also conducts inspection of selected offices and shares findings with the DoP.

572. *Rural banks:* NABARD performs offsite surveillance covering some AML/CFT aspects and on-site inspections in particular for its larger institutions. Inspection reports are shared with RBI.

573. *Insurance and pensions*: Supervision planning by IRDAI and PFRDA is based on prudential considerations and AML/CFT aspects are generally covered as a part of prudential on-site inspections. PFRDA inspected approximately 5% of entities in 2022/23, and supervised entities are also required to undergo external audit, covering AML/CFT aspects as well. This appears to be commensurate the risk that these sectors represent.



*FIU-IND (VASPs)*

574. FIU-IND has developed and maintained a detailed risk-profile matrix for registered VASPs, which includes factors such as geographic, product and entity risks. Using the matrix, FIU-IND analyses threats and vulnerabilities (i.e., VASP profile and type of VAs, source of funding of the VASP firm, operational features, economic impact, criminal accessibility), and mitigation measures (of the entire sector, VASP specific measures as well as measures of involved FIs and DNFBPs). On that basis, FIU-IND categorised two VASPs as high risk, 12 as medium, and 14 as low risk. FIU-IND has conducted on-site inspection of the two high-risk VASPs and offsite of seven of the medium-risk entities over the last nine months. The supervision SOP defines the level of engagement with each category following a risk-based approach (annual offsite/onsite inspections and biannual review meetings for high-risk VASPs; biennial inspections and annual review meetings for medium-risk VASPs, and inspections every three years and review meetings every two years for low-risk VASPs). Whilst FIU-IND adopts a risk-based approach to supervision, supervisory staff appears limited (i.e., consisting of three FTEs), in particular taking into account the complexity and growing nature of the sector.

*DNFBPs*

575. Risk-based supervision of DNFBPs is varied with the supervisors of professionals (mostly high-risk sectors) at setting up stages and therefore yet to begin AML/CFT compliance monitoring following their recent designation as AML/CFT supervisors. On the other hand, the REA supervisor has undertaken compliance monitoring activities, though they are recent and covered a small fraction of the sector. Inspections on real estate agents and casinos revealed that compliance improvements with TFS, BO and STRs requirements are needed.

576. *Professionals*: Supervisors for professionals were designated in May 2023 and therefore risk-based supervision is work in progress as demonstrated by their efforts of building dedicated supervision capacities. AML/CFT on-site and off-site inspections have not commenced.

577. *Real estate*: The supervisor for real estate agents developed a risk-based profile, issued in November 2023 based on which it can risk rate its supervised population and determine the ones to be prioritised for inspection. Under the profile, high-risk REAs include the ones that have not registered with FIU-IND, not appointed Principal officer and Designated Director, REAs dealing with clients in blacklisted countries, among other factors. Inspections are based on an 18 AML/CFT point check list, including items such as designation of a principal officer, maintenance of customer and transaction records, AML/CFT training, and TFS processes. There is a dedicated tax audit team (151 auditors) for covering the AML/CFT aspects of the checklist as well. CBIC has inspected 114 of real estate agents in the period from 2022 to June 2023. This represents a small fraction of the sector composed of approximatively7 000 REs.

578. *Casinos*: Casino supervisors apply risk-based procedures and have sufficient staff for supervision and monitoring of compliance. There is dynamic and closer monitoring of the casinos through quarterly returns and weekly onsite bilateral engagements made possible by the small size of the sector. They check compliance with the AML/CFT requirements by casinos in line with the guidelines issued.

579. *DPMS*: Where DPMS providers fail to observe prohibitions relating to cash transactions in the income tax act, this may lead to a penalty in the amount of cash received. However, no penalty can be imposed if a person proves that there is a 'good and sufficient reason' for the contravention. This provision weakens the legal prohibition, as it is not clear how this clause may be interpreted. Nevertheless, since the cash transaction restriction is monitored for tax purposes, it is covered in external audit reports (prepared by an external accountant) and in tax inspections. Approximately 50 DPMS were identified per year (during the period 2017-2020) not observing the prohibition, but no information was available on how many DPMS were checked to determine a compliance rate. Overall, this appears a low number given the number of DPMS in India (c. 175 000).



### *Remedial actions and effective, proportionate, and dissuasive sanctions*

580. FI supervisors use a range of remedial actions to enforce AML/CFT requirements. The focus has been mainly on educative measures, and monetary penalties, when imposed, are generally not proportionate or dissuasive, in particular for larger firms. Business restrictions that have been imposed by RBI (e.g., prohibition to onboard new customers, withdrawing MVTS licenses) in selected occasions appear dissuasive. Although most FI supervisors can impose sanctions on both individuals and REs (power to remove key managerial personnel), the practice has been to focus on only sanctioning the entities. In addition to the statutory supervisors, FIU-IND has conducted enforcement action against REs that commit serious systemic failures. that has raised the effectiveness of the overall sanctioning regime to some extent.

581. For the VASP sector, FIU-IND has started applying remedial actions. In the DNFBP sector, supervisors have made limited use of remedial actions to date.

#### *RBI (Banks, OFIs)*

582. RBI has a range of remedial actions at its disposal to promote compliance. After each inspection, supervisors share supervisory findings with the entity's board (whether banks or NBFCs) or directors (OFIs). An inspection report is also issued, highlighting the issues for the entity to address. The supervision department can also demand that the entity makes corrective measures under a given timeframe, as well as issue letters of displeasure, warnings, advice the entity to undergo a special audit with a third-party auditor (e.g., for an audit of its IT system), or impose a restriction on its business activities, such as onboarding new customers until an issue is addressed. Those measures are applied depending on the importance of the breach, in line with RBI's supervisory matrix.

583. Since 2017, RBI's enforcement department is responsible for verifying if there are "actionable offences" and if so, for issuing monetary penalties (except for violations in relation to foreign exchange, which is dealt by the foreign exchange department). The enforcement department follows up on the supervision findings, elaborates its own report for each inspection and decides whether to take enforcement action, considering the seriousness and extent of violations and any aggravating factors (e.g., repetition of a serious violation). A decision is made by a three-member adjudication committee and the process, which takes a maximum time of 16 weeks, involves hearing the affected FI. The RBI can also suspend or ultimately revoke a business's licence.

584. The system provides for checks and balances. The enforcement department takes an independent decision from supervision and can decide to take enforcement action in response to

failures identified, even if that has not been part of the recommendations made by the supervision team. However, the enforcement department's decision on the significance of the fine appears to be driven on the materiality of failure relative to the size of the institution, rather than a refined consideration of its potential impact.

585. A summary of monetary sanctions imposed on banks and NBFCs during the review period is summarised in the table below:

### Table 6.7. Details of penalties imposed by RBI on Banks and NBFCs for AML/CFT violations

| Financial Year | Commercial Banks | | Cooperative Banks | | NBFCs | |
|---|---|---|---|---|---|---|
| | No. of entities | Total Amount | No. of entities | Total Amount | No. of entities | Total Amount |
| 2018-19 | 8 | INR 81 million (EUR 900 621) | 4 | INR 1.6 million (EUR 17 790) | - | - |
| 2019-20 | 12 | INR 62 million (EUR 689 364) | 2 | INR 1.1 million (EUR 12 230) | - | - |
| 2020-21 | - | - | 4 | INR 1.3 million (EUR 14 454) | - | - |
| 2021-22 | 2 | INR 12.5 million (EUR 138 984) | 52 | INR 14.6 million (EUR 162 334) | 4 | INR 1.90 million (EUR 21 125) |
| 2022-23 | 5 | INR 24.85 million (EUR 276 301) | 20 | INR 6.9 million (EUR 76 719) | 3 | INR 2.95 million (EUR 32 800) |

Source: RBI

586. The average monetary penalty applied by the RBI was EUR 80 000 for commercial banks, EUR 4 000 for co-operative banks and EUR 8 000 for NBFCs. The failures leading to these sanctions appear to have been at least moderate violations (e.g., failure to categorise customers into different risk categories; lack of robust systems to monitor suspicious transactions; CDD failures). Some examples demonstrated repetition of failures from one supervisory cycle to another, raising questions on the overall dissuasiveness of the remedial actions applied.

587. The RBI only has powers to sanction supervised entities, and not the individuals in charge or those responsible for the violations, with the exception of powers to remove key managerial personnel. This power has not been applied in connection with AML/CFT failures during the review period and should be considered to improve the dissuasiveness of the regime, in particular in case of serious violations.

588. The case below is a good example of RBI imposing sanctions for serious failures.

#### Box 6.3. Sanctions to X Bank Ltd

The RBI conducted an offsite AML/CFT risk assessment of Bank X. The assessment revealed that the bank was outlier in many criteria if compared with other banks, leading to concerns regarding its AML/CFT controls.

The RBI conducted a special AML on-site scrutiny of Bank X. In view of the concerns identified, in March 2022, the RBI directed the bank to stop on-boarding of new customers

with immediate effect till further guidance from RBI. The RBI also directed the bank to appoint an IT audit firm to conduct a comprehensive system audit.

In October 2023, the RBI imposed a monetary penalty of INR 53.9 million (EUR 599 300) on the bank for deficiencies in regulatory compliance. All sanctions were made public in RBI's website.

Source: RBI

589. For OFIs, the average monetary penalties were lower e.g., EUR 550 on average for FFMCs, which would reflect the smaller size of these entities in comparison to the other sectors. However, FFMC failures ranged from non-compliance with cash transaction limits, to failures in CDD and risk categorisation of customers and monetary penalties imposed (ranging from EUR 100 to EUR 1700), appear very low and are unlikely to be dissuasive even for small businesses. The table below includes the financial penalties applied during the review period:

### Table 6.8. Details of penalties imposed by RBI on MVTS and PSOs for AML/CFT violations

| Financial Year | No. of entities inspected | No. of entities found violating | No. of entities on which penalty was imposed | Total penalties imposed |
|---|---|---|---|---|
| **Full Fledged Money Changers (FFMC)** | | | | |
| 2018-19 | 653 | 12 | 2 | INR 20000 (EUR 222) |
| 2019-20 | 593 | 29 | 3 | INR 40 000 (EUR 445) |
| 2020-21 | 452 | 43 | 8 | INR 631 000 (EUR 7 015) |
| 2021-22 | 705 | 33 | 13 | INR 529 000 (EUR 5 881) |
| 2022-23 | 606 | 74 | 23 | INR 1 059 500 (EUR 11 780) |
| | | | | |
| **Authorised Dealers Category II – Foreign Exchange** | | | | |
| 2018-19 | 35 | 2 | - | - |
| 2019-20 | 35 | 1 | - | - |
| 2020-21 | 28 | 2 | - | - |
| 2021-22 | 33 | 2 | - | - |
| 2022-23 | 41 | 2 | 1 | INR 367 000 (EUR 4 080) |
| **Payment System Operators (PSOs)** | | | | |
| 2018-19 | 42 | 19 | | Nil |
| 2019-20 | 25 | 21 | | INR 23.90 (EUR 265 738) |
| 2020-21 | 31 | 12 | | INR 18.54 (EUR 206 142) |
| 2021-22 | 45 | 13 | | INR 31.36 (EUR 348 685) |
| 2022-23 | 44 | 11 | Not available | Not available |

Source: RBI

590. On 22 occasions in the review period, RBI also withdrew FFMC licenses for serious AML/CFT failures, and these have had a more dissuasive effect, as illustrated in the case study

below. Non-financial sanctions were also imposed against authorised dealers in foreign exchange. Licences have also been revoked (1 in 2019, 13 in 2020 and 1 2022) where deficiencies had not been rectified. In one case in 2021, the matter has been referred to the ED for investigation.

### Box 6.4. FFMC licence cancellation after snap audit

The RBI conducted an inspection of the FFMC and found five major and two procedural irregularities. The inspection report was closed after the FFMC demonstrated satisfactory compliance. However, as the irregularities observed also included the violation of AML/CFT guidelines, a snap audit of the FFMC was subsequently conducted to verify the measures put in place by the entity. The snap audit observed irregularities, including serious violations of AML/CFT and money changing guidelines and the FFMC was advised to address them. However, the FFMC failed to do so and the RBI requested it to surrender its licence. The RBI also forwarded the case to ED for action.

Source: RBI.

591. The RBI discloses information on more serious penalties imposed to the public at large, including the name of the entity and AML/CFT violations, in press releases. This is a helpful deterrent to both the individual entity and the wider supervised sector, as it signals RBI's expectations in terms of compliance.

*Other FI supervisors (SEBI, IFSCA, IRDAI, PFRDA, NABARD and DoP)*

592. *Securities:* SEBI and stock exchanges have the power to impose a range of sanctions, from advisory letters and warnings to suspension and cancellation of licencing/registration and monetary penalties for ML/TF offences. During the review period, most infractions led to the issuance of advisory or warning letters. Where monetary penalties were imposed, they were generally not proportionate or dissuasive to the type of violations observed (e.g., inadequate CDD at the time of account opening, lack of update of AML policy, failure to apply EDD to high-risk clients, absence of mechanisms to deal with alerts, failure to appoint a principal officer). On the basis of the case studies provided, monetary penalties did not exceed the equivalent of EUR 5 000. SEBI expressed caution on the use of more severe sanctions due to the negative reputational impact these measures may have on firms, as sanctions are published in SEBI's website. The FIU also imposed sanctions on securities firms for systemic failures (see sub-section below).

### Table 6.9. Inspections by exchanges and depositories and AML/CFT violations observed

| Financial Year | No. of AML/CFT violations | No. of penalties were levied | Total penalty amount | No. of deficiency letters/ warnings issued |
|---|---|---|---|---|
| **Inspections by stock exchanges** | | | | |
| 2018-19 | 115 | 32 | INR 1 025 000 (EUR 11 396) | 85 |
| 2019-20 | 55 | 10 | INR 105 500 (EUR 1173) | 37 |
| 2020-21 | 10 | 2 | INR 54 500 (EUR 605) | 6 |
| 2021-22 | 2 | 0 | - | 2 |
| 2022-23 | 2 | 0 | - | 3 |
| | | | | |

| Financial Year | No. of AML/CFT violations | No. of penalties were levied | Total penalty amount | No. of deficiency letters/ warnings issued |
|---|---|---|---|---|
| **Inspections by depositories** | | | | |
| 2018-19 | 92 | 5 | INR 2 850 (EUR 32) | 88 |
| 2019-20 | 121 | 11 | INR 52 000 (EUR 578) | 115 |
| 2020-21 | 30 | 6 | - | 30 |
| 2021-22 | 47 | 4 | - | 47 |
| 2022-23 | 42 | 6 | INR 35 000 (EUR 389) | 23 |



### Box 6.5. SEBI Adjudication Order: BOI Shareholding Limited –Depository Participant

During inspection and post inspection analysis, SEBI found the depository participant (DP) to be in violation of AML/CFT requirements, in particular:

- The DP did not check the names of existing clients against the UN sanction lists.
- The DP's AML/CFT policy did not incorporate the requirements of the SEBI AML/CFT circular and did not include provisions relating to tipping off, procedure for freezing of funds, procedure for carrying out enhanced due diligence where required.
- The DP did not categorise its clients according to riskAnd did not have a separate alert generation mechanism of its own and took into account the alerts generated by other depositories on a fortnightly basis.

In view of the violations observed, the adjudicating authority imposed a penalty of INR 0.4 million (EUR 4 450). The Securities Appellate Tribunal has subsequently observed that the appellant had implemented all the required AML/CFT policies and procedures as stipulated under the various SEBI circulars.

Source: SEBI

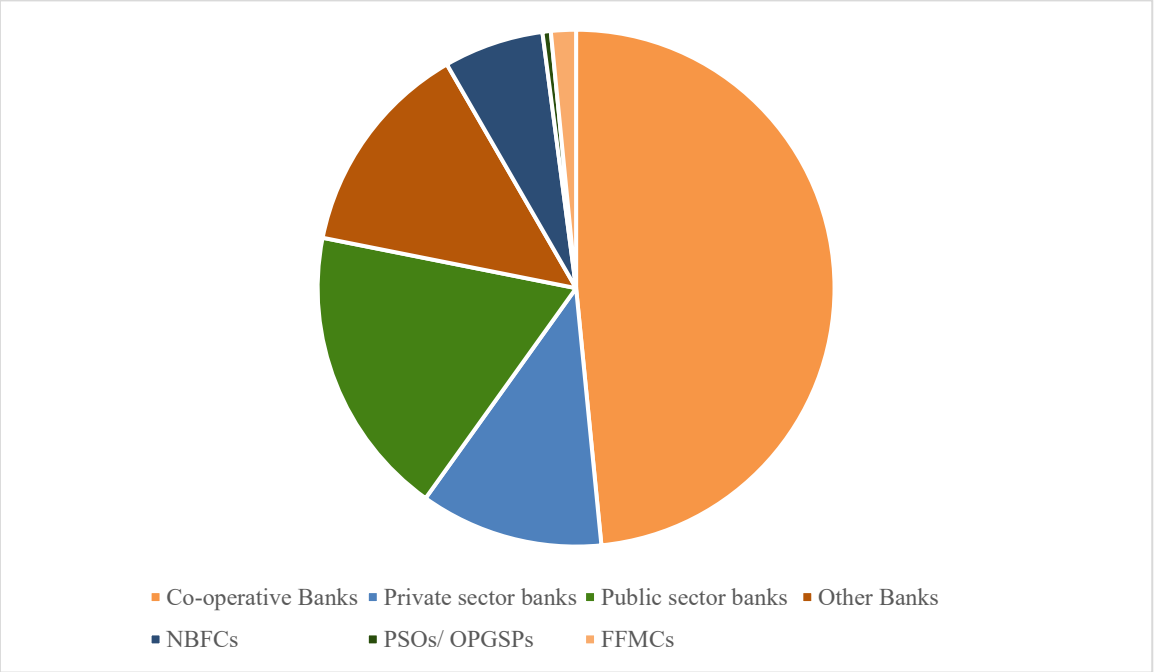
593. *Other FI sectors:* For the insurance sector, IRDAI applied remedial actions, but no monetary sanctions for AML/CFT violations observed during the review period. In some instances, FIU-IND applied sanctions on insurance companies for violations in STR reporting among other failures. PFRDA has neither applied sanctions nor remedial actions to the pension sector as it has not identified any serious AML/CFT violations. For the international financial centre, *IFSCA* has observed a small number of instances of non-compliance since starting to conduct inspections in 2022 and has issued cautionary letters to IFSC reporting entities in response. The *DoP* has undertaken disciplinary actions against officials for AML/CFT failures *NABARD* does not have the power to impose sanctions but has referred cases to RBI and FIU-IND for sanctioning.

*FIU-IND*

594. In addition to the supervisors, FIU-IND also has powers to apply sanctions on any RE for AML/CFT violations under the PMLA. Supervisors generally refer cases of systemic failures they encountered to FIU-IND for enforcement action. FIU-IND can also proactively apply sanctions on the basis of its own findings without relying on a supervisor's initiative. There have been cases where FIU-IND and supervisors (RBI and SEBI) applied sanctions to the same institution.

595. From January 2018 to November 2023, FIU-IND conducted 71 compliance actions based on the regulator's referral and 131 actions based on its own initiative. Most action refer to cooperative banks (93), followed by private and public banks, although sanctions applied in the public and private banks were higher, indicating the severity of deficiencies found. The full set of entities is included below:

### Figure 6.1. Type of FIs subject to compliance action by FIU-IND




Source: FIU-IND

596. FIU-IND imposed sanctions where deficiencies were identified, including cases of systemic failures to file STRs or cash transaction reports, or to conduct CDD, including beneficial owner identification as well as lack of internal controls (for generating alerts or reviewing them). Those were published on FIU-IND's website. So far, FIU-IND's monetary sanctions focused only in the financial sector and no sanctions were imposed in the DNFBP sector yet. Details are included in the table below.

### Table 6.5. Details of regulatory actions on REs by FIU-IND for AML/CFT violations

| Financial Year | No. of cases warning issued | No. of cases penalty imposed | Penalty imposed |
|---|---|---|---|
| 2018-19 | 14 | 1 | INR 0.3 million (EUR 3335) |
| 2019-20 | 4 | 13 | INR 194.6 million (EUR 2 163 714) |
| 2020-21 | 50 | 17 | INR 15 million (EUR 166 781) |
| 2021-22 | 32 | 8 | INR 1.84 million (EUR 20 458) |
| 2022-23 | 14 | 10 | INR 23.33 million (EUR 259 401) |

Source: FIU-IND

597. The following case study provides a good example where FIU-IND undertook enforcement action, after LEA reported failures in AML/CFT controls of a large bank.

### Box 6.6. Failure to report suspicious transactions by a foreign MNC bank

FIU-IND received First Information Reports (FIRs) by a state police force in relation to certain companies alleged conducting and facilitating of online gambling. Proceeds of such criminal activities were routed and channelled through the bank accounts maintained by the same entities in MNC Bank.

After becoming aware of the above FIRs, the bank filed STRs with FIU-IND in respect of the referenced accounts as well as accounts of others affiliated entities. FIU-IND performed further scrutiny on the STRs, called for additional information and observed that MNC Bank: (i) may have closed alerts generated relating to the accounts of the above referenced entities improperly; (ii) may have failed to conduct effective due diligence in connection with the same accounts despite large transactions observed; and (iii) may have failed to put in place an effective mechanism to detect and report suspicious transactions.

On account of such shortcomings, the Director of FIU-IND levied a penalty of INR 20.67 million (EUR 229 825) and along with specific and detailed directions to the bank to take corrective actions in a time-bound manner to mitigate the risks of similar occurrences in the future.

Source: FIU-IND

*VASPs*

598. FIU-IND has applied remedial actions to follow-up on its on-site and off-site inspections, which revealed some shortcomings in ML/TF risk management. On-site supervision revealed some issues for remediation including travel rule implementation, risk categorisation of customers, EDD process for high-risk customers and filing of STRs. Off-site exercises also identified issues for remediation, such as the integration of red flag indicators into alert generation system and methodology, and processes for identifying higher risk customers and wallets. VASPs were asked to, for instance develop a nuanced categorisation of customers based on NRA, SRAs and institution specific RA; implement the 'travel rule' for VA transfers; and complete EDD for high-risk customers. FIU-IND has set a timeframe for issues identified through its supervision to be addressed, and if the VASPs fail to report progress by then, further sanctions including monetary penalty or suspension would be considered. No sanctions had been applied by the time of the ME onsite visit, which was only eight months after FIU-IND commenced its supervision work. Therefore, the effectiveness of remedial actions could be assessed only to a limited extent.

*DNFBPs*

599. Enforcement actions against AML/CFT failures have been applied on casinos and real estate agents by their respective supervisors, most in the form of follow-up. Since no inspections were conducted on professionals (mostly high-risk), no enforcement actions have taken place either. Furthermore, there is insufficient information where inspections were conducted for comprehensive assessment of the scope and risk levels of the entities to which remedial actions and/or sanctions were applied. In general, the supervisors prefer to apply informal and collaborative remedial actions which include outreach activities, bilateral meetings and feedback on remediation.

### *Impact of supervisory actions on compliance*

600. Most FI supervisors demonstrated that supervisory intervention in their respective sectors is having a positive impact on compliance. In the VASP and DNFBP sectors, due to the recency of most supervisory frameworks, it was difficult to demonstrate the impact of the supervisory actions.

*FIs*

RBI (banks, OFIs)

601. The RBI maintains regular communication with commercial banks and larger NBFCs and UCBs. This includes staff following up with the entities following inspections until they are satisfied that any shortcomings have been remedied. The RBI observed that violations are generally not repeated over time, that shortcomings are becoming less severe and FIs are investing more in compliance. Deficiencies identified have been resolved through follow-up inspections apart from a small number of foreign exchange dealers, whose licences were revoked by the RBI. The table below shows RBI's assessment of FI's actions to address deficiencies identified.



**Table 6.6. Details on AML/CFT deficiencies raised and corrected**

| | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| **Banks** | | | | | |
| Number of banks with AML/CFT deficiencies identified during on-site inspection, scrutiny, etc. | 78 | 63 | 46 | 45 | 61 |
| Number of banks found to have corrected AML/CFT deficiencies in compliance submitted by REs or in follow-up inspections | 78 | 63 | 46 | 45 | 61 |
| **FFMCs and Authorised Dealers Category II – Foreign Exchange** | | | | | |
| No. of cases where deficiencies were identified during on-site inspection, scrutiny, etc. | 13 | 23 | 38 | 16 | 46 |
| No. of cases deficiencies corrected (in compliance submitted by REs or in follow-up inspections) | 13 | 22 | 25* | 15 | 45 |

602. Specific campaigns focusing on periodic updates of KYC CDD updates and identification of mule bank accounts also generated tangible results. Following a thematic review that identified deficiencies in periodic updates of KYC CDD , banks were advised in February 2023 to address the issue and progress is monitored on a regular basis. This exercise resulted in significant reduction in CDD pendency, even if pendency numbers for high-risk customers continue to be high (see table below). Banks have also imposed restrictions on the use of accounts by customers that have not been cooperative with efforts to update customer information. The RBI continues to closely monitor progress and has sanctioned banks that presented systemic failures in this area.

**Table 6.7. CDD Pendency in commercial banks**

| Risk Profile | Low | Medium | High | Total |
|---|---|---|---|---|
| March 31, 2022 | 1.16% | 4.50% | 20.25% | 2.19% |
| June 30, 2023 | 0.20% | 1.13% | 10.61% | 0.62% |
| Sep 30, 2023 | 0.17% | 0.93% | 9.33% | 0.53% |

Source: RBI

603. For FIs whose supervision falls outside the Department of Supervision (in particular some entities in the MTSS scheme), it is unclear if the same positive trend in respect of AML/CFT compliance is being observed.

*Other FI supervisors (SEBI, IFSCA, IRDAI, PFRDA, NABARD and DoP)*

604. Supervisors for securities and insurance sectors (SEBI and IRDAI) presented case studies to demonstrate how their actions resulted in improvement of their REs' compliance with AML/CFT obligations; however, without more information on the extent of supervisory findings over time, it was difficult to reach a definitive conclusion. IFSCA supervisory engagement is very recent, and no information was provided to demonstrate their impact on IFSC FI's compliance. Other FI supervisors (NABARD, DoP) could not provide sufficient information to demonstrate the impact of their actions in the sectors they supervise.

*VASPs*

605. FIU-IND engages very closely with the VASP sector providing guidance, developing red-flag indications, engaging in offsite and onsite inspections, providing feedback on STRs and outreach and training. Since FIU-IND's close engagement with the sector as it was being brought within the AML/CFT framework, over 750 STRs have been filed by VASPs. These have led to the identification of various typologies on cybercrime, TF, child sexual abuse material, cross border remittancesand identity fraud. However, the impact of FIU-IND's actions on compliance by VASPs is difficult to demonstrate, due to the recency of its supervisory actions, as at the time of the ME on-site visit, FIU-IND did not have the opportunity to verify if remedial actions have resulted in VASPs addressing issues identified in inspections,.

*DNFBPs*

606. Casino supervisors closely monitor compliance through weekly returns, bilateral meetings and review of progress reports on remedial actions. The rest of the DNFBP supervisors did not demonstrate that they had in place and had applied monitoring tools for assessing changes in compliance behaviour of regulated entities due to less supervisory coverage of the DNFBP sector as a whole. It is therefore difficult to draw conclusions on compliance trends of inspected entities. However, there are positive compliance trends observed in respect of risk assessments and AML/CFT controls such as compliance function with senior and general compliance officers and screening for TF sanctions and PEPs as DNFBP sectors become integrated into the AML/CFT framework.

## *Promoting a clear understanding of AML/CFT obligations and ML/TF risks*

607. Supervisors are actively conducting outreach activities with their sectors, with a different focus depending on the supervisor and level of maturity of the sector. Activities are very recent in most DNFBP sectors, also due to the recent appointment of supervisors. FIU-IND has performed an important role in promoting REs' understanding of reporting obligations and ML/TF risks. FIU-IND has developed red-flag indicators for different sectors, shared information on key typologies (e.g., TBML, cyber-enabled frauds, cash withdrawals by foreign cards at sensitive locations) and established a public-private partnership to share information on typologies and risks which have all had a positive impact on risk understanding in respective regulated sectors.

*FIs*

RBI

608. The RBI has published AML/CFT guidance, conducted outreach activities, including workshops and training events, and issued advisory letters to support the implementation of AML/CFT obligations. Through its frequent engagement with supervised entities, in particular banks and larger FIs, RBI has promoted a clear understanding of AML/CFT obligations. Interviewed

FIs noted the clear feedback they receive following offsite and onsite inspections and their very frequent engagement with their RBI supervisor manager who is available on an on-going basis to discuss questions or concerns, citing direct access to FIU staff in case of questions and the helpful feedback or letters of appreciation they received from the FIU in respect to submitted STRs as examples of communication that helped them understand and implement their AML/CFT obligations.

609. The RBI may consider the need for a more tailored and targeted approach to certain categories of firms with which it currently has less frequent engagement. As the AML/CFT supervisor of a large universe of FIs – more than 13 000 authorised entities of different sizes, complexity and ML/TF risk profiles – RBI may wish to balance outreach activities across all sectors it supervises, with a focus those with higher ML/TF risks and needs, such as sub-sectors of the MVTS sector (e.g. MTSS), in order to promote a clear understanding of their obligations and the risks they are exposed to.



Other FI supervisors (SEBI, IFSCA, IRDAI, PFRDA, NABARD and DoP)

610. All FI supervisors undertake a range of outreach activities to promote an understanding of ML/TF risks and obligations. SEBI, IFSCA, IRDAI and PFRDA have issued sector-specific AML/CFT guidelines. SEBI has also developed and delivered a Certified AML Manager Course and trained 304 participants as of September 2023. DoP has engaged with different post offices across the country for awareness raising. It was not clear if the selection considered any previous findings in relation to compliance with AML/CFT aspects. NABARD is working to ensure REs have systems and alerts in place (e.g., for TFS screening) and other internal controls, as well as compliance with CDD and record keeping obligations. FIU-IND has organised a workshop for NABARD supervised entities. NABARD's ability to promote a clear understanding appears to be limited at the present stage and it is still developing its AML/CFT understanding and supervisory framework.

*VASPs*

611. FIU-IND has conducted a large amount of outreach, feedback and guidance on compliance and identifying and remedying violations of ML and TF risk management, as the sector has been recently introduced into the AML/CFT framework. For example, since VASPs became reporting entities in March 2023, FIU-IND has organised 11 training and outreach sessions, meetings of the working Group on red-flag indicators, as well as 10 one-to-one meetings on typologies and feedback on the quality of STRs (VC meetings) with individual VASPs. The WG on RFIs is a public-private partnership, which includes stakeholders from VASPs and FIs like payment gateways and banks, that collects, analyses and assesses red flags relative to customers, products/services, typologies, etc. A sub-group was also created on peer-to-peer transactions and cybercrimes to identify risks associated with them. For example, at the onset of being brought under the purview of the PMLA and its rules, FIU-IND held a meeting with the VASPs briefing them on their role and obligations for sanction screening with respect to TF and PF TFS and sharing case studies regarding the identification and freezing of accounts.

*DNFBPs*

612. DNBFPs supervisors collaborate closely with FIU-IND on their outreach activities, a positive feature as newer supervisors are able to draw on the experience of FIU-IND working with regulated entities on improving STR reporting. This is most evident when issuing guidance and conducting outreach andawareness raising activities at bilateral and industry levels. The efforts took place through in-person and virtual trainings, publication of guidance, sharing of risk indicators and training material placed on the websites of the FIU-IND and some supervisors or industry

associations. The entities interviewed were aware of and provided positive feedback on the guidelines and awareness-raising and training conducted. For instance, in June 2023 FIU-IND has issued guidance for company secretaries and accountants which are supervised by SRBs. However, there has not been sufficient outreach across all sectors (e.g., lawyers). In addition, outreach in relation to TF TFS obligations (see Immediate Outcome 10) or in relation to the NRA findings as the NRA is not public (see Immediate Outcome 1) has been insufficient, owing to the large size of most DNFBP sectors and the recency of the AML/CFT supervisory framework.

## Overall conclusion on IO.3

Licensing, registration and fitness and probity checks to prevent criminals from entering the financial, VASP and DNFBP sectors are broadly adequate, except for DPMS. There are, however, insufficient checks to identify criminals owning or being a beneficial owner of some types of FIs in the foreign exchange sector. Checks for criminal associates are insufficient in sectors such as foreign exchange and securities, VASPs and some DNFBPs.

RBI, the financial supervisor of the most material sectors, generally has a good understanding of inherent ML risks and a reasonable understanding of TF risks and adopts a risk-based approach to supervision of banks, which is important given the materiality and risks associated with the sector. The supervision of MVTS (PSOs and MTSS, a type of MVTS identified in the NRA as posing TF risks), remains challenging, as the sector relies on subagents with mixed level of understanding and application of preventive measures.

For the VASP sector, whilst risk-based supervision has commenced, supervisory capacity appears limited considering the complexity and growing nature of the sector. For the DNFBP sector, supervision is less developed (except for casinos) and supervisors are building capacity to supervise and monitor compliance with the obligations by the sectors including in high-risk sectors. The shortcomings identified for high-risk professionals and real estate agents were weighted heavily, considering their risk and materiality.

Financial sanctions imposed by FI supervisors were generally limited in number and value. Business restrictions imposed by RBI in a case of systemic failures appear more dissuasive. The enforcement action by the FIU-IND against FIs that committed serious systemic failures in STR reporting has raised the effectiveness of the sanctioning regime to some extent. There has been a strong focus on outreach and promoting REs' understanding of reporting obligations and ML/TF risks across the sectors.

As a result of a restriction on cash transactions above a set threshold under tax law, the DPMS sector falls outside the scope of preventive measures. However, it is unclear whether the sector has been sufficiently monitored for compliance and whether the penalty provisions are dissuasive. As such, there are doubts as to whether the ML/TF risks in the sector are sufficiently mitigated by the cash threshold prohibition. This has been weighted heavily considering the size and materiality of the DPMS sector and its importance in the context of India.

India is rated as having a moderate level of effectiveness for IO.3.

# Chapter 7. LEGAL PERSONS AND ARRANGEMENTS

## Key Findings and Recommended Actions

## Key Findings

a) Information on the creation and types of legal persons and legal arrangements is publicly available in India. There is a centralised portal for information on the creation and types of legal persons, whilst information on some legal arrangements is available mainly at state level.

b) India has a good understanding of the inherent vulnerabilities associated with different types of legal persons and legal arrangements, demonstrated through the 2022 NRA, the 2023 sectoral risk assessment (SRA) and the mitigating measures taken since its last mutual evaluation. The country has identified private limited companies as the most vulnerable legal person for misuse for ML, in particular through the use of shell companies and complex structures, and charitable/public trusts as the most vulnerable legal arrangement for ML and TF misuse. Both were considered to carry a 'medium-low' residual risk. Nevertheless, the residual risks posed by informal nominee arrangements, which is important in the country risk and context, have not been assessed.

c) India has taken specific mitigation measures to prevent the misuse of legal persons and arrangements. For example, the Ministry of Corporate Affairs (MCA) struck off more than half a million suspected shell companies and the same number of directors. Also, professional trustees and TCSPs including company secretaries have been AML/CFT reporting entities and are since May 2023 subject to CDD obligations.

d) Competent authorities can obtain basic and beneficial ownership (BO) information on legal persons directly from a public registry maintained by the MCA; legal persons themselves, reporting entities through FIU-IND, a Central KYC Registry with CDD information collected by FIs and international co-operation. The MCA public registry contains basic information of legal persons, including information on legal ownership, as well as information on significant beneficial owners (SBOs) for legal persons that declared having a more complex ownership structure, which represent a small proportion of legal persons in India. There are strong features in the registry including the pre-certification of e-filings, regular scrutiny by the MCA and possibility of the public filing complaints about the information contained, to support the adequacy, accuracy and currency of the information. In addition, FIs have commenced filing STRs when identifying discrepancies between the information contained in the MCA

registry and the BO information they collect when performing customer due diligence.

e) Information on legal arrangements is available from a combination of sources. Competent authorities can also access BO information on legal arrangements from reporting entities (including professional trustees) where legal arrangements have a relationship with them, and also from FIU-IND/ Central KYC Registry, when the legal arrangement has a relationship with a FI in India. For public/charitable trusts, information on settlor, trustee and beneficiaries is available with state charity authorities. Tax records also require some basic and BO information to be maintained in in relation to legal arrangements with tax consequences in India.

f) The MCA monitors compliance with annual returns with basic information. On average, over 70% of active legal persons file these returns on an annual basis and legal persons that are repeated offenders face strike off over time. The MCA also monitors filling of returns by nominee/nominators and SBO information. However, it is currently difficult for India to differentiate cases where an entity has no SBOs from the cases where an entity has SBOs but failed to submit a return, even if India has established a structure and processes to identify cases where SBO returns are due.

g) India has sanctioned legal persons for failure to submit returns with basic and SBO information as well as providing false information using a range of measures. This included striking off legal persons that failed to file annual returns and applying administrative fines for late or incorrect returns. However, financial sanctions are not always set at a dissuasive level for larger businesses. Criminal prosecution has also been pursued in limited instances, including when false statements have been submitted. Where gatekeepers were found to be actively involved in administering legal persons engaged in criminal activity, cases were referred to professional bodies or also prosecuted directly; however, there was limited evidence that professional bodies have consistently taken action against the involved professionals. Similarly, there was limited information on sanctions applied in connection to legal arrangements.

## Recommended Actions

a) India should deepen its understanding of the misuse of legal persons for ML/TF, in particular by assessing any residual risks posed by informal nominee arrangements.

b) India should enhance the monitoring of requirements for disclosure of nominators, taking the country risk and context, and in particular the issues around informal nominee arrangements and assess their effectiveness.

c) India should enhance timely access to adequate, accurate and current basic and BO information on legal persons. This could be achieved by:

   a. enhancing the MCA's activities, including the Central Scrutiny Centre's role in reviewing accuracy of basic and beneficial ownership

information;

b. enhancing the awareness of SBO obligations and further monitoring of compliance by legal persons by, for instance, by requiring legal persons who do not have any SBOs to confirm that in their annual returns or establish a similarly effective method;

c. strengthening the mechanism for FIs, DNFBPs and VASPs reporting discrepancies on BO information they identify to FIU-IND or directly to the MCA.

d) India should enhance access to adequate, accurate and current basic and BO information on legal arrangements, by closely monitoring the implementation of AML/CFT obligations by professional trustees.

e) India should enhance the application of effective, proportionate and dissuasive sanctions to ensure accurate and up-to-date information is consistently available on basic and beneficial ownership by:

a. systematically sanctioning the breaches of basic and BO information requirements, including applying dissuasive administrative and criminal sanctions where appropriate; and

b. working with Self-Regulatory Bodies to ensure that they take dissuasive and proportional disciplinary action against their cost and work accountants, chartered accountants and company secretaries that submit false information to the registry and take action directly where appropriate.

613. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.[119]

## Immediate Outcome 5 (Legal Persons and Arrangements)

### *Public availability of information on the creation and types of legal persons and arrangements*

614. There are two types of legal persons in India: companies and limited liability partnerships (LLPs). Information on the creation and types of legal persons is publicly available on the MCA website (www.mca.gov.in). The website contains e-books on the Companies Act, 2013 (CA) and Limited Liability Partnership Act, 2008, along with rules and applicable forms required to be filed for incorporating and maintaining legal persons in India. The MCA also publishes an annual report providing details of the type and number of legal persons registered in the country.[120] As at 3

[119] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

[120] A "registered company" means a company which has been registered in India with the Registrar of Companies at any point of time.. See also: www.mca.gov.in/content/mca/global/en/data-and-reports/reports/annual-reports/annual-report.html

November 2023, there were 2 601 457 registered companies (1 630 411 active, and the remaining struck off by the Registrar, dissolved by the Court or amalgamated by scheme of merger or companies which are under liquidation or under resolution process as per the Insolvency and Bankruptcy Code) and 336 283 LLPs (303 141 active, and the remaining struck off or converted into companies).

615. There are four categories of legal arrangements in India which fall within the FATF Standards: Private Trusts, Charitable or Public Trusts (including wakfs), Societies and Hindu Undivided Families (HUFs). There is no centralised source of information on the different types of legal arrangements and the mechanism for their creation. Such information is provided, however, under the respective statute and governing rules concerning each specific arrangement, which may be at central or state level (or both), depending on the arrangement.[121] For public trusts, wakfs and societies, the respective state registrars maintain information on legal arrangements registered by them in a register.

616. Other forms of businesses in India include partnerships (governed by Indian Partnership Act, 1932) and sole proprietorships (governed by State legislation), both of which do not have legal personality. Partnerships and sole proprietorships are common ways of doing business in India considering the simplicity of their establishment, in comparison with the formalities for companies and LLPs. See Chapter 1 and Immediate Outcome 1.

### *Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities*

617. India has identified and assessed ML/TF risks and vulnerabilities of legal persons to a reasonable extent. This conclusion is based on a review of the various risk assessments produced by India (including the NRA and a specific risk assessment of legal persons and arrangements), discussions with LEAs, regulatory agencies, FIs, accountants and TCSPs; as well as case studies showing the role of legal entities and arrangements in ML/TF cases in India.

618. The risk assessment of legal persons and arrangements was carried out in consultation with respective LEAs and agencies including the ED, MCA, ITD and FIU-IND. The results of this exercise were incorporated in the NRA adopted in November 2022. Further, in March 2023, the Department of Revenue conducted a sectorial risk assessment (SRA) of the vulnerabilities of legal persons and arrangements, and the extent to which they can be or are being used for ML/TF.

619. The NRA concluded that the vulnerability concerning availability and access to BO information was Medium-High. The NRA identifies the use of shell companies as a preferred route for ML involving significant sums, especially for proceeds of fraud offences, corruption and tax crimes. Risks identified included the laundering of proceeds outside India using corporate structures, with a high-risk of dissipation to overseas "secrecy jurisdictions". The subsequent SRA concluded that legal persons and legal arrangements carried the following residual risk (see table 7.1).

[121] Some governing statutes may be available electronically. See www.indiacode.nic.in.

### Table 7.1. Risk assessment of legal persons in India

| Type of Entity | ML Risk | TF Risk |
|---|---|---|
| **Public Companies** | Low | Low |
| **Private companies** | Medium | Low |
| **Limited Liability Partnerships** | Medium Low | Low |
| **Foreign Legal Persons** | Medium High | Low |
| **Private Trusts** | Low | Low |
| **Public/Charitable Trusts** | Medium Low | Medium Low |

620. The SRA focused on the general characteristics of legal persons ("risk profile"), the findings of specific cases ("risk scenarios"), and the mitigating measures in place, to arrive at a rating of residual risk. Private limited companies (PLCs) were found to be the type of domestic legal entities carrying the most risk of misuse for ML, followed by LLPs, because of their characteristics, such as limited liability, separate legal personality, and lack of transparency in their ownership and control structures. The following typologies are highlighted:

- PLCs/LLPs having **complex ownership structures**, with multiple layers of ownership and control, especially with entities from different countries, make it difficult to trace the ultimate beneficial owner and can be used to hide the identity of those who are controlling them. They have been used, for instance, to receive commissions/ kickbacks in corruption cases and also to own real estate and other assets acquired with proceeds from corruption;
- PLCs can be used for **opening offshore accounts** e.g., in tax haven countries to hide the source of funds and evade taxes;
- **Shell companies** – i.e., companies with no real business operations - are considered as particularly vulnerable for ML. There has been a significant rise of incidents in India where shell companies have been used for **illegitimate purposes,** including obscuring the actual ownership of assets, serving as a conduit for siphoning funds from e.g., fraud schemes, illegal gambling, obtaining bank loans by falsification of financial statements and misusing the funds, manipulation of share market prices using circular trading, and holding offshore bank accounts; and
- PLCs were also used to create **complex transactions** (layering/pass-through transactions) and participating in trade-based ML schemes.

621. Public companies were found to carry a relatively lower risk of misuse for ML as they are subject to higher scrutiny from regulators and investors. The misuse of publicly listed companies for ML purposes observed in India mainly relates to instances of market manipulation through artificially inflating or deflating the price of securities. Like for PLCs/LLPs, the use of complex structures involving foreign subsidiaries was also found to make it difficult to trace the flow of funds and identify the ultimate beneficial owners.

622. India has taken several measures to increase transparency of beneficial ownership, applied additional controls for the appointment of directors, and taken enforcement action to strike off shell companies (see 7.2.3 below). Taking into account these measures, it has assessed the residual risk of misuse of PLCs as medium and LLPs as medium-low. The SRA did not elaborate in detail on the impact of mitigation measures in the determination of the residual risk.

623. Some aspects could be further explored by India. In the last five years, only 5% of entities in total have reported having indirect owners (i.e., they are not beneficially owned by their shareholders). It would be useful for India to consider whether there remains a vulnerability related to the use of nominee shareholders and/or directors for concealing beneficial ownership, despite the measures taken in this respect (see also the analysis in section 7.2.3). Whilst India has taken specific legislative measures against strawmen or "benami" ownership of assets in 2016 (see section 7.2.3 below), demonstrating its risk understanding, the effectiveness of these measures in preventing informal nominee holdings of shares have not been assessed yet.

624. The TF risk assessment of legal persons in the SRA is less developed and is based on the lack evidence of the misuse of these structures for TF purposes to draw its conclusions. The experience of LEAs in terrorism and TF cases indicated that companies and LLPs were not a preferred channel for routing funds for terrorist activities, although there was limited analysis of specific features of legal persons (including Section 8 companies, used for charities) that could be prone for misuse for TF, if any.



**Box 7.1. Money Laundering with Shell Companies**

In January 2021, following the filing of a first information report (FIR) with the police of the State of Hyderabad, and subsequent searches, the police undercover a network of persons and mobile applications engaging in micro-lending at exorbitant rates. The applications were operated by foreign individuals through a web of shell companies in India. These applications provided loans to victims at high interest rates, while also collecting personal data of victims from mobile phones, and using the personal data to blackmail victims and recover the loan amount with interest.

The *modus operandi* involved: (i) foreign subjects incorporating shell companies in India to receive money from their home country. These companies had both foreign and locally hired Indian directors. (ii) These shell companies then entered into an MoU with Non-Banking Financial Companies (NBFCs) in India. Under the MoU, they provided security deposits to NBFCs which in turn opened multiple Merchant IDs with payment gateways which allowed the shell companies to run mobile applications. Such applications were listed on major mobile App stores. (iii) Loans were provided through the app, and recovery was done through the app/payment gateway and transferred back to the shell companies by the NBFCs through the Merchant IDs after deducting a commission.

The investigations resulted in Provisional Attachment Orders in the amount of INR 7.8 billion (EUR 87.3million) confirmed by the Adjudicating Authority as well as the prosecution against 521 (legal and natural) persons, which is on-going.

Source: MCA

### *Mitigating measures to prevent the misuse of legal persons and arrangements*

625. India has taken a variety of legislative, administrative and policy measures over the last five years to prevent or mitigate the misuse of legal persons and arrangements and strengthen access to adequate, accurate and up-to-date basic and BO information, which India has achieved to a large extent.

626. The implementation of public registers that hold basic and BO information, as well as requirements on the legal entities themselves are important developments. Another is the

development of a Central KYC register, which contains some CDD information, including BO information on legal persons and arrangements that have an account-based relationship with an Indian financial institution. The operation of the registers and their ability to provide adequate, accurate and current basic and BO information is discussed below in section 7.2.4.

627. In addition, specific mitigating measures have been taken to identify and remove shell companies and other non-compliant companies from the registry of companies. Requirements have also been strengthened in respect of nominee ownership and bearer shares and share warrants (see c.24.11). More recently, the inclusion of professional gatekeepers (accountants, trust and company service providers including company secretaries) as reporting entities subject to CDD and reporting obligations under the PMLA is also a significant development.

*Measures against shell companies*

628. India has taken specific measures to mitigate the use of shell companies, following the 2015 report by the Special Investigation on Black Money. That report recommended a twofold strategy: (i) proactive detection of the creation of shell companies in the company registry by intelligence gathering through regular data mining and dissemination of information to various LEAs for surveillance; (ii) deterrent penal action against persons involved in the creation or management of shell companies engaged in illicit activities.

629. The report's recommendations triggered multiple operational responses. A Task Force on Shell Companies was set up in February 2017 with a mandate to scrutinise the company registry in a systematic way against red flag indicators, developed on the basis of typologies identified by LEAs on the misuse of companies for illicit purposes.

**Box 7.2. Task Force on Shell Companies**

The Task Force on Shell Companies had as key task the compilation of a database comprised of three lists:

1. the Confirmed List included confirmed shell companies based on the information received from the various LEAs of the companies involved in illegal activities;
2. the Derived List included companies identified based on 100% common directorships with the confirmed shell companies; and
3. the Suspect List had suspected shell companies that had been drawn up using the red flag indicators.

Graded strategies, following a risk-based approach, were used to deal with these entities. Over 500 000 companies were struck off as a result in subsequent years. The lists were extensively used by LEAs to conduct investigations and the Registrars of companies at state level for inspections. In certain cases, the involvement of professionals in the operations of confirmed shell companies was detected and cases were brought for prosecution (see below).

Source: MCA

630. The MCA undertook a striking off exercise in 2017-18 in response to the Task Force findings. The Registrar can strike off companies and LLPs when they have failed to commence business within one year of incorporation; when they are not carrying out business or operations for a period of two immediately preceding financial years and have not made an application for dormant status; and when the Registrar ascertains that the company is not carrying out business or operations by

visiting its address. [122] A scheme was brought in 2018 to assist genuine companies regularising their pending returns, resulting in over 14 000 companies regularising themselves and having their names reinstated in the registry. The striking-off exercise continued in the following periods, with some brief alleviation during the COVID-19 pandemic.

### Table 7.2. Number of companies struck off

| Financial year | No of Companies struck off | No. of LLPs struck off |
|---|---|---|
| 2017-18 | 234 357 | 1 169 |
| 2018-19 | 138 432 | 7 397 |
| 2019-20 | 65 162 | 3 551 |
| 2020-21 | 12 887 | 3 752 |
| 2021-22 | 63 246 | 2 847 |
| 2022-23 | 83 017 | 1 774 |

631. The MCA continues to perform checks against red-flag indicators on an on-going basis. Whilst India has taken all the measures as described above to ensure to mitigate risks, the misuse of shell companies remains a high-risk area as per the NRA (see Chapter 1 and Immediate Outcome 1), requiring continued actions.

*Requirements to disclose nominee shareholdings and directors*

632. Over the last ten years, India has introduced mitigating measures to increase transparency of nominee relationships. *Benami* transactions, which broadly refer to circumstances where assets are held or transferred through strawmen, informal nominees, or fictitious persons have been a concern, in particular in the context of real estate transactions (see Chapter 1 and Immediate Outcome 1). There have been two relevant legislative changes.

633. The 2015 amendments to the Companies Act 2013 introduced a requirement for nominee shareholders and nominators to disclose their relationship to the company, as well as for the companies to disclose this information to the Registrar. As analysed in section 7.2.4 below, during the review period, over 9 000 returns on average have been filed on an annual basis, which would approximately refer to less than 0.5% of active companies disclosing a nominee shareholder relationship.

634. The Benami Transactions (Prohibition) Amendment Act of 2016 permits the civil confiscation of assets held in *benami* as well as imprisonment of those involved. This act has been introduced mainly to address known typologies in the context of real estate and other assets held by front persons on behalf of (true) owners, in many cases acquired with money from corruption or other crimes (see Chapter 1). The Income Tax Department has set up 24 dedicated Benami Prohibition Units across India involved in identifying the benami properties and taking enforcement action. Three case studies were presented by India to demonstrate that the powers of this act were also evoked for benami ownership of shares, leading to seizures of the shares involved, but broader statistics on cases during the review period were not available.

635. In relation to directors, in India, only natural persons can be appointed as directors of an Indian company and they must obtain a Director Identification Number (DIN). This requires the provision of a photograph, proof of identify and proof of residence. Companies are required to notify the Registrar of the appointment of a director and their DIN, which permits the Registrar to verify how all directorships an individual holds. Based on the recommendations of the Task Force

[122] Section 248 of the Companies Act, 2013, and section 75 of the LLP Act, 2008.

on Shell Companies, over 370 000 directors were disqualified for non-filing of financial statements or annual returns for a continuous period of three preceding financial years (2013-14, 2014-15 and 2015-16), but this has been less of a focus in recent years (see Table 7.9 in section 7.2.6 below). On disqualification, a director's DIN becomes inactive, and the disqualified director is prohibited from being appointed as a director of any company or from managing the company in which they are already a director, for a period specified in the CA (e.g., 5 years) or until they rectify the reason for disqualification.

*Requirements for professional trustees and other TCSPs*

636. Since May 2023, persons acting as (or arranging for another person to act as) a trustee of an express trust on a professional basis or otherwise acting as a TCSP, have become reporting entities under the PMLA. TCSPs were required to register with FIU-IND. As at November 2023, 36 registrations had been received. In addition, accountants and company secretaries providing services covered by the standard were notified as reporting entities (see more details under IO3 and IO4). Those were important steps considering the role accountants and TCSPs commonly play in company formation and management in India.



## *Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons*

637. India ensures timely access to adequate, accurate and current basic and BO information on legal persons to a large extent. Competent authorities obtain information from various sources: the company registries maintained by MCA; AML/CFT reporting entities, in particular banks; from the FIU-IND, which facilitates access to the Central KYC Registry, containing some CDD information, including BO information collected by financial institutions; legal persons themselves; and international co-operation. Competent authorities also investigate BO by tracing assets, and reviewing contractual relationships and other records (e.g., forensic accounting, review of records maintained by the stamp and registration departments) as part of ML/TF and predicate crime investigations. The MCA registries are a first stop for LEAs who in their investigations would normally attempt to cross check information from multiple sources.

*Public Corporate Registries*

638. The MCA consolidates in one electronic portal (https://mca.gov.in) information from the 27 Registries of Companies (ROCs) that exist across India at state level. The general public can access basic and available BO information after registration and payment of a small fee per each item accessed. Access by LEAs and most other competent authorities is free of charge. Returns can be accessed by searching for a variety of fields (e.g., the name of the legal person or director), but there is no possibility for downloading the entire registry (e.g., for civil society to analyse trends).

Basic information

639. Companies and LLPs electronically file annual returns with basic information, including details of shareholders, partners, indirect holders of beneficial interest in a company (i.e., nominators), directors and designated partners (as well as information on significant beneficial ownership (see further details below). Some information is also required to be filed electronically as soon as there is a change (including information on directors for companies and partners for LLPs, as well as new allotment of shares) and this information is updated in the register as soon as it is received.

640. On average, over 70% of active legal persons file annual returns as indicated in Table 7.3 below.

### Table 7.3. Filing of annual returns (Form No. MGT-7)

| Financial year | No of active companies | No of annual returns received from companies at 31 Dec of the calendar year | Filing rate[123] |
|---|---|---|---|
| 2018-19 | 942 207 | 741 082 | 78.65% |
| 2019-20 | 1 044 475 | 788 579 | 75.50% |
| 2020-21 | 1 159 714 | 858 634 | 74.04% |
| 2021-22 | 1 317 676 | 871 187 | 66.12% |
| 2022-23 | 1 486 427 | 861 221 *(up to the on-site visit in Nov 2023)* | 57.94%[124] |
| **Financial year** | **No of active LLPs** | **No of annual returns received from LLPs** | **Filing rate** |
| 2018-19 | 104 228 | 83 445 | 80.06% |
| 2019-20 | 134 715 | 96 065 | 71.31% |
| 2020-21 | 166 021 | 117 676 | 70.88% |
| 2021-22 | 213 222 | 149 319 | 70.03% |
| 2022-23 | 249 918 | 159 073 *(up to the on-site visit in Nov 2023)* | 63.65% |

641. Newly formed companies are not required to file their first annual return by 31 December of their year of incorporation but are included in the figures for the table above (7.3). An average of 140 000 new companies were formed each year over the review period. Taking out these companies, the actual compliance rate would range from 73 to 90%.[125] In addition, companies were also granted extensions during 2021 and 2022 on account of the COVID-19 pandemic, reducing the proportion of companies required to file annual returns by year end even further. It should also be noted that filing rates for each year continue to increase after the deadline as a result of late filings. Companies that fail to file returns for more than two years will be selected for striking off and penalties apply for late filers (see section 7.2.6). LLPs were also granted an extension to the filing deadlines during the COVID-19 pandemic.

642. There are some strong features of India's regime that support the adequacy, accuracy and currency of information:

- ***Pre-certification of e-filings***: Authorised signatories or practicing professionals (accountants and company secretaries) certify company filings and are responsible for their accuracy.[126] This pre-certification acts as a pre-emptive check to ensure that the information stated in the form or return are as per the books and records of the company and are accurate.
- ***Regular scrutiny of returns*:** The state ROCs perform regular checks to detect defective and inaccurate filings. Checks are performed using different criteria such as failure to file ancillary information where required, mismatch in filings, inputs received from competent authorities, or on the basis of random selection. In addition, MCA's Central Scrutiny Centre scrutinises approximately 0.44% of filings – i.e., out of 8 million

[123] This includes legal persons that filed an annual return by 31 December of the calendar year. It does not include filings made after that date, so late filings are not captured.
[124] This refers to annual returns received up to 10 November 2023.
[125] This refers to returns received during years 2018-19 to 2021-22. For year 2022-23, 65% of returns had been received until the onsite visit (November 2023).
[126] Section 92(1) of Companies Act and Rule 8(12) of the Companies (Registration of offices and fees) Rules, 2014).

filings received in a year, on average, 35 000 filings get scrutinised on an annual basis by the Centre. Electronic checks are conducted against other filed data. Out of those filings, on average, less than 6% (2 000 out of 35 000) are marked as defective and disseminated to state ROCs for action or striking off.[127]

- ***Complaints STRs:*** any person can e-file a "serious complaint form" about a legal person. On average, over 2 000 complaints are received a year, but it is unclear how many of those refer to basic and BO information. They are investigated by MCA and some are shared with LEAs for action. FIs also file STRs where they identify a discrepancy in CDD information with registered information (see section below).
- ***Other means:*** the MCA also receives intelligence from LEAs and regulators on the basis of their investigations, and performs further checks (e.g., visiting the address of legal persons to verify if business in being conducted) which could lead to sanctions or strike-off. This was evidenced by some case studies but no statistics on those checks were available.



Beneficial ownership information

643. There are a set of filing requirements meant to identify beneficial owners, but their monitoring is challenging.

644. Since 2019, companies and LLPs are required to identify their "significant beneficial owners" (SBOs, see c.24.6 and 24.12) and file this information with the Registrar. SBOs, in short, refer to natural persons who own or control a legal person indirectly or by a combination of direct and indirect holdings or have right to exercise, or actually exercises, significant influence or control, in any manner other than through direct holdings alone. That means that natural persons who only directly own and control more than 10% of the shares of a company are not considered SBOs. In addition to SBO filings, nominees and nominators are also required to identify themselves (more details below). Finally, as noted above, legal ownership information is also filed with the Registrar and, as a result, this information would permit identifying all individuals who directly hold shares of a company or are a partner of an LLP.

645. In summary, a comprehensive set of reporting obligations are in place for legal persons to have available and up-to-date information on their beneficial owners, and provide this information to the MCA Registrar:

- Companies are required to take steps to identify their SBOs. This includes issuing a notice (form no. BEN-4) to, at a minimum, legal owners that hold at least 10% of the company's shares or voting rights and are not natural persons;
- Persons who are SBOs to a company are required to inform the company (form no. BEN-1);
- Persons who hold shares of a company but do not hold beneficial interest in such shares are required make a declaration to the company specifying the name and other particulars of the person who hold the beneficial interest in such shares (form no.MGT.4); and

[127] 1521 filings in 2018-2019, 1784 in 2019-2020, 3500 in 2020-2021, 1372 in 2021-2022 and 974 in 2022-2023.

- Persons who hold a beneficial interest in the shares of a company without being legal owners are in turn required to provide a declaration to the company (form no. MGT-5) disclosing such an interest. The company, in turn, files a return informing of such declarations to the MCA Register (form no. MGT.6).

646. Companies are required to maintain a register of SBOs (form no. BEN-3), derived from the various SBO submissions described above, and electronically file this information with the MCA Registrar (form no. BEN-2). The filed forms are publicly available in the MCA website and reflect the information filed by the company itself. Similar requirements apply for LLPs.

647. "Full" BO information would be available through a combination of SBOs information reported by the company (if any) plus the information held on (any) natural persons that would directly hold or control at least 10% of the shares or voting rights of the entity (unless they reported not having a beneficial interest in the company).



648. Concerning monitoring of compliance, there are approximately 2 million active legal persons, and only about 100 000 SBO returns have been filed with the Registrar from year 2019 to year 2023. It is challenging for the MCA to determine whether the remaining 95% of legal persons that have not submitted a SBO return would have a SBO to report but failed to do so, or simply do not have any SBOs. Lack of compliance is easier to spot where a legal person has corporate shareholders or declared nominees, as the MCA can easily identify this information on the basis of annual returns or nominee returns. However, situations of control by other means would be more difficult to spot. One interview with an expert from the private sector also indicated SBO information sometimes included information on legal persons, raising concerns about accuracy of the data. The data on SBO returns received over the last five years is summarised below.

### Table 7.4. SBO declarations furnished by companies to the MCA Registry

| Description | Form No. | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| Number of declarations made by companies in respect of beneficial owners | BEN-2 | 75 525 | 11 810 | 8 741 | 7 253 |

Source: MCA

649. Concerning the declaration of beneficial interest (i.e., nominee ownership), the number of returns has been on average less than ten thousand per year with a small increase in recent years, as per the table below. It is not clear whether this is because there is a low number of nominees or if there are issues with the compliance of filing obligations.

### Table 7.5. Returns by companies to the MCA Registry in respect of nominee shareholders

| Description | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|
| Return to the Registrar in respect of declaration under Section 89 received by the company (MGT-6) | 7 560 | 7 788 | 9 513 | 12 038 |

Source: MCA

650. The MCA monitors compliance following a risk-based approach. Monitoring actions include, in addition to actions described in relation to basic information above (e.g., pre-certification of e-filings):

- ***Cross checking of data to identify missed SBO filings*:** Based on filed annual returns, the MCA identified 50 459 legal persons which have shareholders other than individuals holding 10% of its shares and did not submit a SBO return. The

MCA contacted those companies and (only) 292 legal persons have reported the SBO information subsequently. To further prioritise its resources on a risk basis, MCA narrowed down the list to focus on high-risk cases. On that basis, MCA identified 274 companies where it will prioritise investigation and enforcement action in the future.

- ***Regular scrutiny of returns*:** During the period 2019-2022, 1 032 SBO filings have been scrutinised and out of those only 24 SBO filings were found defective. The SBO information is checked by cross-verifying other basic information available in the registry, such as the layers of holding companies, nature of shareholding and break down of direct and indirect holding of the individual SBO.
- ***Assigning a SBO ID***: A SBO ID is created when a natural person is reported as a SBO for first time and permits identifying all legal persons to which this natural person is an SBO.
- ***Other means***: MCA also acts on the basis of complaints received against companies, ground intelligence, referrals from LEAs etc. FIs also file STRs where they identify a discrepancy in BO information, but this occurred in a relatively small number of instances (i.e., 119 STRs in the review period).

651. Whilst the approach is comprehensive and employs multiple mechanisms that all have a positive impact on the accuracy of filings, the MCA Registry still needs to strive to detect whether natural person shareholders are or are not beneficial owners under the SBO filling system. India needs to enhance the monitoring mechanisms. This is particularly important as the MCA database has been widely used by CAs and are also heavily relied upon by REs for their CDD processes (see IO4). Data on access is included in the tables below (tables 7.6 and 7.7).

### Table 7.6. Number of searches made in MCA Registry via open access

| Description | 2017-18 | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|---|
| Records accessed through MCA website | 2 141 296 | 2 655 055 | 2 955 674 | 3 176 933 | 4 117 397 | 4 453 904 |

### Table 7.7. Number of searches made in MCA Registry by competent authorities

| User | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| RBI[128] | 2 664 | 3 665 | 1 402 | 42 | 55 |
| SEBI | 584 | 905 | 367 | 792 | 459 |
| CBI | 326 | 632 | 332 | 480 | 512 |
| Police | 120 | 758 | 220 | 5 | 325 |
| Official Liquidator | 32 | 1 | 5 | 7 | 76 |
| Other Agencies[129] | 14 137 | 28 343 | 21 800 | 25 657 | 38 683 |
| **Grand Total** | **17 863** | **34 304** | **24 126** | **26 983** | **40 110** |

Source: MCA

[128] The RBI has been mainly accessing the MCA registry via the open access in recent years.
[129] Other agencies include ED, ITD etc.

*Central KYC Registry/ REs*

652. As described in section 5.2.3, reporting entities perform CDD through which they identify the BO of their customers. As of May 2023, accountants, company secretaries and other TCSPs have become AML/CFT reporting entities and are required to identify and verify BO information of their clients. They are also involved in the filing of annual returns and financial statements with the ROC.

653. In addition, legal persons in India commonly engage with an Indian bank or another FI, which are required to perform CDD and submit some basic and BO information they collect to the Central KYC Registry (see section 5.2.3, Immediate Outcome 4). In particular, all active legal persons are required to file annual income tax returns containing their bank account numbers.[130] At as November 2023, the Registry contained records of over 1.896 million non-individual accountholders (Indian or foreign companies, LLPs, trusts, societies etc). FIU-IND has direct access to this information and provides it to LEAs upon request, or proactively if FIU-IND identifies concerns. This provides competent authorities with timely access to BO information collected by FIs in the CDD process, without the need to engage FIs or accountholders.

654. As noted in Immediate Outcome 4, FIs heavily rely on the MCA registry to identify and verify BO information of Indian legal persons, so to which extent the Central KYC Registry provides a truly separate source of BO information is to be verified. A positive feature is that FIU-IND's red flag indicators include the circumstance where an FI identifies discrepancies in BO information collected from CDD and the data available in the MCA Registry. During the review period, 119 STRs were filed in relation to this. In addition, BO identification has been identified as a supervisory focus by RBI, the bank supervisor, over the last two years (see Immediate Outcome 3).

*LEAs' use of investigative powers*

655. LEAs have powers to obtain any information from any person and thus rely on multiple sources to uncover basic and BO information in their investigations. The MCA registries are a starting point as they provide a quick and direct method of searching for basic and available BO information. Depending on the case and the information already in their possession, LEAs will also seek BO information from records, maintained by legal persons themselves, CDD information from reporting entities, international co-operation and other inquiries on assets and contractual relationships to identify whether control is held by other means by any person. LEAs have been successful in uncovering beneficial ownership in complex structures using a multi-pronged approach to identify Bos (See Box 7.3 below).

**Box 7.3. Case Study: Misuse of legal persons for Money Laundering in Corruption Case**

CBI registered a criminal complaint under the provisions of the Prevention of Corruption Act, 1988 against a sitting Cabinet Minister, Mr. AB, of the Delhi Government. The complaint alleged that Mr. AB had acquired disproportionate assets through corruption while holding public office and had laundered the illicit proceeds through shell companies in India beneficially owned by him.

The investigation revealed that during Mr. AB's tenure as Cabinet Minister from February 2015 to May 2017, INR 48.1 million (EUR 535 000) proceeds of corruption in cash was received by companies W, X, Y, and Z, managed and controlled by him, and accounted as "bogus entries" in the companies' account books. The shell entities were incorporated solely

[130] Income tax form ITR6 combined with section 187 of Companies Act, 2013.

for the purpose of converting cash into legitimate funds through methods such as high premium share capital or unsecured loans, with a commission fee of approximately 1-2%.

Mr. AB initially held either 100% ownership or majority shareholding in the companies W, X, Y, and Z. Upon becoming the Cabinet Minister, Mr. AB divested his shareholdings in the companies to his wife. He resigned from official positions but continued managing and controlling the companies through dummy directors, who were his friends.

Mr. AB sought the assistance of a chartered accountant who facilitated the bogus accounting entries through hawala operators, who in turn transferred the funds to other shell company operators. Through multiple layers of transactions, the funds eventually reached companies owned by the accused, and agricultural lands were purchased using the funds.

BO information was determined based on various sources including corporate filings, bank records and CDD documents, Land Revenue records and use of the PMLA powers to obtain information, documents and statements from chartered accountants and hawala operators.

To conceal the source of the entries, Mr. AB declared the funds as undisclosed income under an Amnesty Scheme introduced by the Government of India in 2016, which allowed individuals to disclose unaccounted income for tax purposes. Statements from the dummy directors, the chartered accountant and shareholders were important to identify Mr. AB's beneficial ownership of the entities.

Mr. AB was arrested on 30 May 2022 and is currently in judicial custody. Prosecution complaints under PMLA have been filed against him, and his properties have been attached. In total, 6 properties worth INR 48.1 million (EUR 535 00) has been attached. The trial is in progress.

Source: ED

### *Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements*

656. India ensures timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements to a large extent. Information on legal arrangements is available from a combination of sources including state charity authorities in relation to public trusts, tax records for legal arrangements with tax consequences in India, trustees and the Central KYC Registry when the legal arrangement has a relationship with a FI in India.

657. In relation to public trusts and societies, competent authorities rely on information from the registers maintained by state charity authorities, state registers (e.g., wakf registers), and information filed with the ITD for legal arrangements with tax consequences in India:

- ***Tax records***: the Central Board of Direct Taxes maintains a public database[131] of around 280 000 (as of June 20, 2023) tax exempted institutions. The database contains searchable details such as name, address, PAN and unique registration number. At the time of application for a PAN, trustees are required to submit a copy of the trust deed, containing information on the settlor, trustee and beneficiaries. The statutory requirement for availing exemptions includes the furnishing of tax returns, maintenance of books of accounts, their audit by a chartered accountant, and furnishing of audit report at the time of filing of return of income by the trustee.

[131] https://incometaxindia.gov.in/Pages/utilities/exempted-institutions.aspx

Public trusts and societies can be subject to a tax inspection. During the period 2018-2023, 30 276 of public trusts and societies were subject to an audit under the Income Tax Act.

- ***State records***: States have a record of charitable trusts and societies registered in that state as well as other information (e.g., information on settlor, trustee, beneficiaries) required by each state. Some states (e.g., Maharashtra) also have an electronic record[132] with some basic details (name of the trust/society, address, date of registration) available to the public.
- ***Darpan portal***[133]: this portal serves as a database of non-governmental organisations in India. As of November 2023, there were over 185 000 organisations registered in the portal (85 298 societies and 69 160 trusts), which is searchable by sector or state. Through the Darpan portal, registered organisations receive a unique ID. When on-boarding these organisations as clients, FIs are required to register the client details in the Darpan Portal as well.[134] Whilst the portal does not contain beneficial ownership information, there is some basic information about the arrangements and other information can be requested from other parties (such as trustee, FI etc).

658. State charity authorities which regulate charitable/public trust and societies verify the information provided by the legal arrangements and take action where the information is not updated or is not provided. The remedial action for breaches is generally the termination of registration of the legal arrangement. The following table provides the data on the verification of cases and action taken by one state authority, Maharashtra Charity Commissioner during the FY 2018-19 to FY 2022-23. Whilst other States may be carrying out similar activities, no information was available in this respect.

### Table 7.8. Verification / action taken by Maharashtra Charity Commissioner

| Particulars | Type of Legal Arrangement | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|---|
| Number of cases where verifications of the basic information/BO carried out | Trusts | 8451 | 5 258 | 4 122 | 376 | 4 310 |
| Number of cases where verifications of the basic information/BO carried out | Society | 7 775 | 5 618 | 4 397 | 4 406 | 6 482 |
| Number of cases where action was taken for not updating the information | Trusts | 22 | 10 | 28 | 10 | 7 |
| Number of cases where action was taken for not updating the information | Society | 184 | 110 | 99 | 55 | 37 |

Source: Maharashtra Charity Commission

659. For private trusts, CDD obligations imposed on reporting entities (mainly banks, securities firms) and tax records are the main source of legal and BO information. TCSPs have only been recently included in India's AML/CFT regime (in May 2023) and the effectiveness of the regime could not be ascertained; however, some professional trustees that are in the banking or security sector had obligations in place for a longer period (see more details under IO3 and IO4).

660. Information on trusts managed by non-professional trustees is difficult to estimate. Data from tax returns indicated that there are approximately 107 000 active private trusts with tax

[132] https://charity.maharashtra.gov.in:8060/dashboard.aspx
[133] https://ngodarpan.gov.in/
[134] PML Rules, Rule 9(9A).

consequences in India. The top 1 380 trusts (1.3%) constitute approximately 95% of total reported income by trusts in India. India considers that these trusts would usually be trusts managed by professional trustees, and as such the income reported by other private trusts would be limited.

661. HUFs (see Chapter 1) are considered as persons in the PMLA. This means that reporting entities must identify and verify the BO of the HUF, whenever they have an interaction with an FI or DNFBP. In addition, HUFs are treated as a separate entity for taxation purposes under the Income Tax Act, 1961. The tax obligations for an HUF include filing annual income tax returns, paying taxes on income earned by the HUF, and adhering to all compliance requirements prescribed under the Income Tax Act. Every HUF is required to obtain a Permanent Account Number (PAN), which serves as a unique identifier for the HUF in all financial transactions and tax-related matters. The PAN application and related documents provide information on the Karta the head of the HUF (the trustee), and all the coparceners (beneficiaries) of the HUF.

662. There were relatively few ML or TF cases identified in India involving legal arrangements during the review period. During the course of investigations, LEAs usually use multiple sources to identify the parties to a trust. The sources included CDD information, information available with registrars, the PAN registration data and the annual income tax return data provided to the ITD.



**Box 7.4. Case Study: Access of beneficial information of legal arrangement – case of undisclosed funds**

A search and seizure action under the Income Tax Act, 1961 (s.123) was carried out in the investigation of Mr. AB. During the search, evidence of substantial undisclosed foreign assets of the family of Mr. AB was found, which were held either directly or indirectly but controlled by the family.

Beneficial interest in six trusts were held by the family through various entities across the globe for purposes of tax evasion. Funds were routed through various entities, held by a relative of Mr. AB, a non-resident Indian, while Mr. AB and family were the beneficial owner. Mr. AB's relative has been used to transfer funds from one entity to another entity to avoid detection by the Indian tax authorities due to his non-resident status.

The evidence collected in India was corroborated with information collected through exchange of information on the basis of tax treaties with foreign jurisdictions. This includes the trust deed, information on the trust structure and financials, financial records from a company held by the trust as well as correspondence between Mr. AB's family and the trustees. This information confirmed that settlors of one of the trusts and beneficiaries were the members of AB family. Prosecution under section 50 of Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 has been launched against Mr. AB.

Source: ITD

### *Effectiveness, proportionality and dissuasiveness of sanctions*

663. India has implemented effective, proportionate and dissuasive sanctions to some extent. The corporate registrar has struck off legal persons that failed to file their financial statements or annual returns for a continuous period of two or more financial years. The registrar also applied monetary fines (see table 7.10) to legal persons for failure or late filing of basic and beneficial ownership information. In addition, some instances where legal persons had been used for criminal purposes have led to prosecutions for the provision of false information to the registrar. Whilst

some case studies have been presented in connection with these cases, whether dissuasive and proportionate sanctions are applied systematically in serious instances of non-compliance could not be demonstrated.

664. As referenced in section 7.2.3 above, India has struck off more than half a million legal persons which had not filed their financial statements or annual returns for a continuous period of two or more financial years in the company registry. Legal personality ceases to exist after strike-off. A gazette notification of dissolution is issued and published on the e-gazette portal and MCA portal after the expiry of the time mentioned in the notice, the company is considered dissolved. ROCs have a mechanism to inform the Indian Bank Association of the striking off of a company to ensure that its bank accounts are frozen. State governments are also informed and can use this information to restrict the transfer of immoveable property.

665. Actions were also taken against directors associated with fraudulent companies, including actions for disqualifications, so that these persons do not act as director of other companies in India. The statistics of disqualification of directors are presented below. These actions were more strongly taken during the work of the Task Force of Shell Companies, and there is no information on whether this drive has continued since 2022.

### Table 7.9. Disqualification of directors

| Financial year | No of directors disqualified |
|---|---|
| 2017-18 | 31 776 |
| 2018-19 | 376 500 |
| 2019-20 | 91 041 |
| 2020-21 | 34 552 |

666. Table 7.10 below shows the prosecutions and financial sanctions applied by MCA in the last five years for all instances of non-compliance combined, not only those related to the filing of basic and beneficial ownership information. Overall, a small number of cases of non-filers led to prosecutions, and most prosecutions refer to cases of false information or statements:

### Table 7.10. Prosecution and fines on companies

| Description | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|
| **No. of companies prosecuted during the year** | 958 | 591 | 1 103 | 1 636 | 1 532 |
| **Total Fine Imposed (INR)** | INR 39 783 699 (EUR 442 000) | INR 52 430 392 (EUR 582 560) | 14 386 150 (EUR 160 000) | INR 10 462 407 (EUR 116 250) | INR 70 453 955 (EUR 782 800) |
| **Average fine** | INR 41 528 (EUR 464) | INR 88 714 (EUR 992) | INR 13 043 (EUR 146) | INR 6 395 (EUR 72) | INR 45 988 (EUR 514) |

Source: MCA

667. Overall financial sanctions applied appear low. While they might be dissuasive for some natural persons or small businesses, they are less dissuasive for larger businesses or more serious failures.

668. India considers that the financial penalties are dissuasive and proportionate and are imposed with an aim to increase the compliance rate. MCA aims at maintaining a balance between its role as regulator and compliance facilitator. In this context, instances of procedural non-compliance (i.e., failure to file a return without a clear fraudulent intent) attracts less severe punishment. On the other hand, there are more stringent provisions to curb fraudulent conduct – e.g., whether non-filing is done with the intention of manipulation or concealment of vital financial

irregularities or practices would attract criminal prosecution. In instances where the filing of documents, forms, or returns are found to contain false or misleading information or a material omission, the ROC regional director or the Registrar would conduct an inquiry into the professionals or authorised signatory who certified the relevant form. If misconduct is determined, the Registrar submits a complaint to the SRB where the professional is a member and debars the concerned professional from filing any document on the MCA portal in future. In more serious cases, the MCA would also submit the case for prosecution. The table below (Table 7.11) contains statistics on relevant disciplinary actions undertaken in respect of accountants and company secretaries in the last five years.

### Table 7.11. Complaints referred to SRBs

| Financial Year | Number of complaints referred to SRBs | Number of Actions taken by SRBs on referred professionals | Number of prosecutions against Professionals by MCA |
|---|---|---|---|
| 2018-19 | 20 | 0 | 32 |
| 2019-20 | 11 | 3 | 65 |
| 2020-21 | 8 | 0 | 48 |
| 2021-22 | 805 | 12 | 56 |
| 2022-23 | 90 | 1 | 76 |
| **Total** | **934** | **16** | **277** |

Source: MCA

669. Whilst the MCA refers a significant number of cases to professional bodies, in particular following the COVID-19 pandemic, the number of disciplinary actions taken by the professional bodies themselves (ICAI, ICSI and ICMAI) against their members remains low, raising questions on whether accomplice professionals are being adequately disciplined.

670. ROC's actions have been instrumental in undercovering a fraudulent scheme involving thousands of companies (see case below). However, the overall number of prosecutions and convictions was not available, resulting in the assessment team not being able to ascertain the overall effectiveness of the sanctioning regime.

### Box 7.5. Case Study: Verification of information by the ROC

In March 2023, the ROC's Central Registration Centre, while performing regular scrutiny checks on incorporations, identified that a chartered accountant had used fabricated bank statements and proof of address for incorporating a company. The ROC further identify that the accountant had already used the same fake address to incorporate multiple companies and she had also been appointed as the statutory auditor for over 300 companies, including M/s XYZ and its group companies which were in the news for defrauding the public in an amount over INR 21 billion (EUR 233.6 million).

The ROC then executed a search and seizure operation, conducted in the registered office of the audit and legal firm ABC Pvt Ltd in Chennai, as well as the residence of the chartered accountant. It busted a racket for forgery and creation of fake documents for incorporating over 1 500 companies all over India including M/s XYZ. During the raids, ROC seized physical documents and various electronic gadgets, computers which were used for the creation of fabricated and forged documents. About 50 employees associated with the portal were also investigated.

Since then, the ROC has stepped up its watch on chartered accountants and audit firms concerning the filing of forged corporate documents with MCA. Many of these companies were found to be involved in money laundering and other serious financial crimes, including fraud, and some have lured the public to invest in fraudulent schemes.

Source: MCA

671. In relation to legal arrangements, there was insufficient evidence to conclude whether there were effective, proportionate and dissuasive sanctions against persons that failed to comply with the information requirements. In relation to charitable/public trusts, state charity commissioners could terminate registration due to lack of observance of information disclosure requirements (e.g., for Maharashtra trusts); however, no data was available in relation to such actions during the review period.

672. Where a trust or other legal arrangements with tax consequences in India fails to submit a return, financial sanctions also apply. The number of sanctions imposed during the review period for legal arrangements were as below (Table 7.12).

### Table 7.12. Number of sanctions imposed on legal arrangements for failure to provide an income tax return

| Financial Year | Number of penalties imposed |
|---|---|
| 2019 | 149 |
| 2020 | 52 |
| 2021 | 383 |
| 2022 | 558 |
| 2023 | 391 |

Source: ITD

673. The financial sanction is set in the amount of INR 5 000 (EUR 56) plus an assessment of income due if a return is not provided where requested. This sanction is not set at a dissuasive level for most cases.

## Overall conclusion on IO.5

India has demonstrated a good understanding of the inherent vulnerabilities associated with different types of legal person and arrangements through recent risk assessments, although there is a need for India to better assess the residual risks posed by informal nominee arrangements, which is important in the country risk and context, and the effectiveness of mitigating measures put in place in this regard.

India has taken a number of positive steps to enhance transparency of legal persons and arrangements. Those include conducting an intensive campaign to remove shell companies, and implementing a public registry of direct ownership information as well as "significant beneficial ownership" information of legal persons that have declared having a more complex and control structure, although this represents a small fraction of companies in India. The country has also put in place a registry containing BO information of legal persons and arrangements that have a relationship with an Indian financial institution collected via CDD. On legal arrangements, information is available with state charity authorities, tax authorities, or professional trustees; however, the fragmented way information is being kept in relation to public trusts and the very recent CDD obligations for professional trustees limited the assessment of effectiveness to some extent.

Overall, Indian competent authorities have been able to access basic and BO information, relying on a multiple sources of beneficial ownership information. There has been a focus on striking off non-compliant as well as shell companies which has a positive impact in maintaining the integrity of the MCA registry. However, the small amount of the financial sanctions imposed and limited number of prosecutions may not have the dissuasive effect needed to avoid non-compliance in the future. Those issues require moderate improvements.

India is rated as having a substantial level of effectiveness for IO.5.

7

# Chapter 8. INTERNATIONAL COOPERATION

## Key Findings and Recommended Actions

## Key Findings

a) India has a legal framework for MLA that enables it to provide a wide range of assistance, primarily through bilateral and multilateral agreements with all key jurisdictions and regular engagement with these partners to further enhance relationships. India has recently taken steps to improve the coordination and timeliness of response to requests for international cooperation by introducing and implementing updated guidelines and an online portal for coordination and prioritisation.

b) Extradition processes are adequately coordinated through the MEA which receives and disseminates a relatively small number of requests across multiple agencies.

c) Seeking formal international cooperation where appropriate is a standard component of ML/TF investigations in India, with relevant LEAs provided training on seeking assistance from foreign counterparts and this is reasonably sought to pursue criminal assets. Requests have been made in keeping with India's risk profile, but some improvements could be made to the quality of these requests.

d) A number of outgoing MLA and extradition requests remain pending, preventing the finalisation of a number of investigations, prosecutions and confiscations in India, with Indian authorities continuing to follow-up these requests.

e) LEAs and FIU-IND proactively seek informal cooperation with foreign counterparts, largely through membership in regional and international networks. This cooperation has assisted authorities in India in advancing ML and TF investigations.

f) India prioritises the provision of assistance to foreign counterparts with FIU-IND spontaneously disseminating information and responding to all informal requests for information during the last five years, including basic and beneficial ownership information. LEAs also respond to the majority of requests for assistance and have sought to develop closer relationships with strategic foreign partners.

g) Financial supervisors have sought and provided international cooperation to differing extents, with a focus on the provision of information related to fit and proper checks, including basic and beneficial ownership information.

## Recommended Actions

a) India should complete implementation of the new MLA portal to streamline processes and facilitate coordinated and timely execution of requests, including a clear framework for prioritisation.

b) India should provide additional training and guidance to staff tasked with preparing requests for formal international cooperation to improve the quality of these requests specific to the requirements of the requested country.

c) India should improve the system for monitoring incoming and outgoing extradition requests, including by considering applying some of the processes implemented for incoming and outgoing MLA requests, to manage any increase in the volume of requests.

d) Supervisors of entities with international exposure, particularly RBI and IFSCA, should establish or maintain relationships and proactively seek and enhance international cooperation with key foreign counterparts on supervisory matters, including ensuring there is a sufficient legal basis to do so.



674. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

### Immediate Outcome 2 (International Cooperation)

675. In general, India is not an attractive destination country for criminal proceeds, relative to the size of its economy and population, although cross-border risks for ML and TF (with funds moving into and out of the country) are present. India has established relationships with counterparts who represent key trade and commercial relations, financial ties, prevalence of Indian diaspora and historical linkages. In addition to these, jurisdictions with major financial institutions and tax secrecy provisions, represent a large portion of India's international cooperation efforts through established formal mechanisms as well as more informal agency-to-agency cooperation.

#### *Providing constructive and timely MLA and extradition*

676. India's framework for international cooperation is based on a series of bilateral and multilateral agreements, international conventions and on the basis of reciprocity. The Central Authorities for MLA (MHA) and extradition (MEA), and the primary investigating agencies (CBI and ED) have dedicated units and processes in place to respond to MLA requests and key performance indicators that encourage them to respond to requests in a timely manner and provide the widest range of assistance. Although feedback from the global network was generally positive, some countries indicated that responses to requests had not always been timely and communication on the progress of their requests neither regular nor transparent. During the period under review, India has implemented a number of reforms to processes, such as the revised 2019 MLA Guidelines, establishment of a 'desks' system and the introduction of the MLA portal in 2022 to improve timeliness and coordination of requests.

*Mutual Legal Assistance*

677. The MHA operates numerous 'desks', i.e., teams allocated to certain regions/countries to coordinate incoming and outgoing MLA requests with relevant agencies and foreign counterparts, with oversight and coordination at the Director level. The MHA is also supported by the International Police Cooperation Unit (IPCU) within CBI in the transmission of requests through to the nodal office of the relevant law enforcement agency for response, following a review at the MHA level. At times, these requests are sent to multiple agencies simultaneously, with the consent of the requesting jurisdiction. Monitoring of requests is also conducted through monthly reviews, quarterly coordination meetings and biannual meetings as set out in Sections 2.5-2.7 of the MHA Guidelines.

678. India treats each incoming request as a priority, with the highest priority afforded to ML/TF requests involving collection of digital or perishable evidence, criminal intelligence which could be acted upon within India, terrorism cases, and high-risk crimes in which there is an imminent threat to life and public safety. The level of priority for all other requests is established at the central level and communicated through the assignment of request to the relevant LEAs through the MLA portal with a special priority mark. There are no specific SOPs or policy documents in place which explicitly determine how the central team prioritise different types of requests.

679. The MHA also works closely with the International Police Coordination Cell (IPCC) of the IPCU to provide guidelines, SOPs and training to LEAs on providing international cooperation on MLA through formal and informal channels. This training is conducted through the relevant law enforcement academies and regular conferences, as required, for nodal officers of relevant state and central LEAs. ED, CBI and NIA also provide specific courses to officers at varying levels on international cooperation, MLA and extradition, and officers also participate in regional and international training programs on international cooperation.

680. As per Table 8.1 below, India has received 719 MLA requests and executed 518 of these during the period under review. During the period under review, responses to MLA requests took on average 355 days.[135] These response times have reduced from an average of 480 days in 2018 to 255 days in 2022 which may be attributable to the introduction of the online MLA portal, as well as other facilitating measures such as the revised 2019 MLA Guidelines and establishment of a 'desks' system, taken through the review period, including training. The response time of specific requests varied depending on the complexity of the assistance sought, the priority afforded to the request and the need to consult with multiple agencies. Overall, the timeliness of responses has improved over the period. Only one incoming MLA request was refused during the period, as insufficient information was available to support a criminal investigation.[136] Responses by the ED to MLA requests related to ML and/or asset seizure also reduced significantly from an average of over 1 000 days in 2018, to 195 days in 2022 and ranged from a response time of 1.5 months to over a year. This demonstrates improvements to processes and prioritisation, particularly by the ED, in responding to ML-related requests for assistance by foreign counterparts.

681. The MLA portal was introduced in December 2022 to further reduce the time taken to respond to requests and improve coordination of responses to these requests. The online portal has had a significant effect on the efficiency of the system. The online transmission of requests from MHA to the relevant LEAs has significantly reduced the substantial time of transmission (as compared with delivery through physical means), as well as the number of channels for processing and execution of requests. The standardisation and digitalisation of records, as well as in-built

[135] 2020 statistics have been excluded from the calculation of this average due to the nationwide lockdowns imposed during that year.

[136] This refers to one of the ML/asset forfeiture requests received in 2018 which was refused in 2021 – see Table 8.1 below

monitoring tools, has improved the end-to-end processing timelines and prioritisation of requests, although India should continue with the set of facilitating measures (above) to ensure the sustainability of improvement. Relevant law enforcement officials at the Central and State levels, including all INTERPOL liaison officers, have been trained in the use of the portal and continue to provide feedback on additional improvements to improve timeliness and coordination of responses.

### Table 8.1. Incoming MLA requests

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (till Nov.) | TOTAL |
|---|---|---|---|---|---|---|---|
| **Number of Requests received** | **93** | **115** | **120** | **115** | **126** | **150** | **719** |
| - of which predicate offences | 25 | 29 | 26 | 28 | 26 | 32 | 166 |
| - of which ML/asset seizure | 2 | 4 | 12 | 9 | 9 | 11 | 47 |
| - of which TF | 0 | 1 | 0 | 0 | 0 | 1 | 2 |
| **Number of Requests executed** | **87** | **104** | **114** | **97** | **91** | **25** | **518** |
| - of which predicate offences | 25 | 29 | 26 | 23 | 16 | 8 | 127 |
| - of which ML/asset seizure | 1 | 4 | 11 | 9 | 9 | 1 | 35 |
| - of which TF | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| **Number of Requests withdrawn** | **5** | **11** | **3** | **6** | **13** | **1** | **39** |
| - of which predicate offences | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| - of which ML/asset seizure | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| - of which TF | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Number of Requests refused** | **1** | **0** | **0** | **0** | **0** | **0** | **1** |
| - of which predicate offences | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| - of which ML/asset seizure | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| - of which TF | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Number of Requests pending** | **0** | **0** | **3** | **12** | **22** | **124** | **161** |
| - of which predicate offences | 0 | 0 | 0 | 5 | 10 | 23 | 38 |
| -of which ML/asset seizure | 0 | 0 | 1 | 0 | 0 | 10 | 11 |
| - of which TF | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

682. India has provided a range of assistance in response to MLA requests. These include the provision of bank records, company records and statements of witnesses, which were required in almost half of all requests in 2023. India has also assisted in attachment (seizure) of proceeds of crime on seven occasions between 2018 and 2022 and has repatriated proceeds to other countries on the one occasion in which the requesting jurisdiction provided a confiscation order, as set out in the case study below.

### Box 8.1 Case Studies: International Cooperation

International Cooperation with the UK

A request was received from the UK in May 2014 to freeze assets held by Mr A in Goa and Bangalore regarding alleged fraud by false representation. This request was forwarded to authorities in Goa who obtained the necessary court orders to seize these assets in November 2014. Two fixed deposit accounts to the value of INR 8 041 463 (EUR 89 350) were seized in April 2015 and a further account in the amount of INR 8,278 (EUR 92) seized in June 2015, which was reported to the MHA for onward transmission to the UK in September 2015.

A supplementary request was received from the UK in August 2018 for the execution of confiscation orders regarding these seized assets. Execution of these orders was approved in India by the court in November 2019 with GBP 78 339 (EUR 91 601) transferred to UK authorities in May 2021.

International Cooperation related to Terrorist Financing

A Note Verbale was received in 2019 from the Embassy of Türkiye seeking assistance in relation to a designated terrorist organisation. The suspect Mr. XXX, one of the militants of the organisation acting in India, had a bank account in YYY bank in India which was used by the terrorist organisation to finance its activities. He was found to have invested a large sum of money in his account in January 2014 and in September 2014 in accordance with the instruction of the head of the terrorist organisation.

The Chief Public Prosecutor's Office's requested to examine and record the statement of a person named Mr. XXX residing in Delhi who was suspected to be a member of the terrorist organisation, in connection with a terrorist attack in 2016. The statement of suspect Mr. XXX was recorded as per the queries of Turkish authorities and the Execution Report along with supported documents viz. balance sheet of the company, Income Tax Report (ITR) of the company, ITR of Mr. XXX and other relevant documents were forwarded to them through Embassy of Türkiye in New Delhi within four months of receiving the request.

*Extradition*

683. The MEA, through the dedicated section within the Consular, Passport and Visa Division, coordinates incoming and outgoing extradition requests with MHA, relevant agencies and overseas missions. The MEA utilises an internal case management system to monitor the status of requests which is sufficient given the low volume of requests currently sent and received.

684. The MEA also collaborates with the IPCC of the IPCU to provide guidelines, SOPs and training to law enforcement agencies on responding to extradition requests. This is supplemented by training provided by ED, CBI and NIA as part of their specific courses on international cooperation, MLA and extradition.

685. As seen in Table 8.2 below, out of 98 extradition requests received by India in the period under review only five related to ML, one of which was subsequently withdrawn. Of all these extradition requests, six have been granted, none of which related to ML. For the four pending incoming extradition requests, three are pending at various stages and one has been returned for further information. India has not received any extradition requests related to TF. Although an example of execution within 10 months has been presented on a non-money laundering request, in

general the process to grant an extradition in relation to any offence takes over a year to be fully executed.

### Table 8.2. Incoming extradition requests

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (till Nov.) | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests Received | 19 | 19 | 21 | 14 | 15 | 10 | 98 |
| ML | 0 | 0 | 2 | 0 | 2 | 1 | 5 |
| No. of persons requested | 21 | 22 | 22 | 20 | 20 | 11 | 116 |
| ML | 0 | 0 | 2 | 0 | 7 | 2 | 11 |
| Requests executed | 1 | 1 | 2 | 2 | 0 | 0 | 6 |
| ML | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Requests withdrawn | 4 | 2 | 1 | 0 | 1 | 0 | 8 |
| ML | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| Requests refused | 7 | 11 | 8 | 0 | 1 | 7 | 34 |
| ML | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| No. of persons extradited | 1 | 1 | 2 | 2 | 0 | 0 | 6 |
| ML | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Requests Pending | 7 | 5 | 10 | 12 | 13 | 3 | 50 |
| ML | 0 | 0 | 1 | 0 | 2 | 1 | 4 |

Note: The figures under the year column denote the number of requests received in that year and the status of the events (execution, withdraw, refusal) in respect of these requests though it may have happened either in the same year or in subsequent years.

## *Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements*

686. During the last 5 years, India has actively sought formal international cooperation in relation to TF, ML and asset recovery requests in the course of their investigations. Of the 282 MLA requests related to ML, 31 have been granted, with a further 241 pending final execution. For these pending requests, partial information has been obtained for three-quarters of requests and Indian authorities have undertaken a range of follow-up measures, including through liaison officers and consular dialogues to seek finalisation of these requests. In addition, for approximately one-quarter of these pending requests, Indian authorities have not received a response from the requested country. Feedback from a small number of jurisdictions indicated some MLA requests had insufficient justification for the measures sought and that requests overlapped at times.

### *Mutual Legal Assistance*

687. The requests made by India are largely in keeping with the ML/TF risk profile, with 96% of all requests relating to fraud and corruption. Although the low number of requests associated with drug trafficking are not commensurate with the identification of this as one of the predicate offences with the most significant ML risks in the NRA, those requests that were made related to serious transnational drug trafficking and associated ML. Drug LEAs, such as NCB and DRI, also focus on more expedient informal cooperation from relevant foreign counterparts in the course of their investigations.

688. Of the 282 MLA requests made relating to ML and TF, 85% remain pending. However, partial responses were received in 70% of such pending requests. Improvements to the quality of these requests, in particular through inclusion of elements specific to the requirements of the requested country, standardised templates and enhanced coordination between domestic competent authorities as supported by the developed MLA portal, may expedite responses to these requests. Ten of the 282 MLA requests, as per Table 8.3 below, made by the ED have been refused, representing less than four percent of all requests. The reasons for these refusals have been identified as being due to the requests being investigatory in nature and more suited to informal cooperation, lacking a nexus between the alleged offence and the requested assistance, or that the records or funds were no longer available.

### Table 8.3. Outgoing MLA requests

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (till Nov.) | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests Sent | **190** | **213** | **105** | **130** | **197** | **148** | **983** |
| ML/asset forfeiture | 68 | 79 | 30 | 41 | 49 | 15 | 282 |
| TF | 3 | 4 | 2 | 3 | 0 | 4 | 16 |
| Requests executed | **38** | **25** | **16** | **15** | **5** | **2** | **101** |
| ML/asset forfeiture | 8 | 10 | 5 | 5 | 3 | 0 | 31 |
| TF | 2 | 1 | 0 | 0 | 0 | 0 | 3 |
| Withdrawn | **10** | **7** | **1** | **1** | **0** | **1** | **20** |
| ML/asset forfeiture | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| TF | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Refused | **5** | **1** | **2** | **4** | **2** | **0** | **14** |
| ML/asset forfeiture | 2 | 1 | 2 | 3 | 2 | 0 | 10 |
| TF | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Pending | **137** | **180** | **86** | **110** | **190** | **145** | **848** |
| ML/asset forfeiture | 58 | 68 | 23 | 33 | 44 | 15 | 241 |
| TF | 1 | 3 | 2 | 3 | 0 | 4 | 13 |

*Extradition*

689. Only one of the 33 ML-related extradition requests and one of the 22 TF-related extradition requests have been granted during the period under review, with the majority of remaining requests still pending. Indian authorities continue to engage with foreign counterparts to finalise the execution of these requests. Eight ML-related extradition requests have been refused by a small number of countries. Feedback from a small number of jurisdictions, including some with pending extradition requests from India, indicated some extradition requests had insufficiently detailed information to meet the legal requirements of the requested jurisdiction and the timeliness of responses to requests for clarification or further information could be improved. Indian authorities continue to engage with counterpart Central Authorities to address their specific requirements for the admissibility of evidence and how information is presented in the extradition requests concerned. In a few cases where the legal requirements have been met and extradition recommended by courts, the extradition is still pending due to undisclosed confidential legal matters, impacting the ability of Indian authorities to successfully conclude prosecutions in India.

### Table 8.4. Outgoing Extradition requests

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (till Nov.) | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests Sent | **34** | **52** | **20** | **19** | **45** | **27** | **197** |
| ML | 8 | 15 | 3 | 0 | 6 | 1 | 33 |
| TF | 1 | 10 | 4 | 4 | 0 | 2 | 21 |
| No. of persons requested | **34** | **54** | **20** | **19** | **45** | **30** | **202** |
| ML | 8 | 15 | 3 | 0 | 6 | 1 | 33 |
| TF | 1 | 11 | 4 | 4 | 0 | 2 | 22 |
| Requests executed | **2** | **3** | **2** | **4** | **2** | **0** | **13** |
| ML | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| TF | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| Withdrawn | **2** | **1** | **0** | **0** | **1** | **0** | **4** |
| ML | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| TF | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Refused | **2** | **8** | **3** | **2** | **1** | **1** | **17** |
| ML | 1 | 7 | 0 | 0 | 0 | 0 | 8 |
| TF | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| No. of persons extradited | **2** | **3** | **2** | **4** | **2** | **0** | **13** |
| ML | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| TF | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| Pending | **28** | **40** | **15** | **13** | **41** | **26** | **163** |
| ML | 6 | 7 | 3 | 0 | 6 | 1 | 23 |
| TF | 1 | 10 | 4 | 3 | 0 | 2 | 20 |

*Asset Recovery*

690. The Indian authorities have also sought international cooperation for asset recovery and have made a number of requests for the attachment of property overseas. Table 8.5 below details the value of requests for attachment/seizure of assets overseas, of which 15 requests involving INR 10 786.1 million (EUR 119.85 million) have been executed and the assets seized, which represents 7.6 per cent of all attached assets located abroad where requests have been made. India has identified challenges associated with the recovery of assets located overseas, especially in relation to non-conviction-based confiscation (NCBC) requests where countries may be unwilling to repatriate assets in the absence of a conviction and has sought to overcome those challenges through alternative measures (see IO.8).

**Table 8.5. ED Requests for attachments sent overseas, 2018-2023**

| Country | Total Attachments | Direct Proceeds | Value Based | Amount Attached in INR Millions | Amount Attached in EUR Millions |
|---|---|---|---|---|---|
| UAE | 8 | 4 | 4 | 2,486 | 27.5 |
| UK | 7 | 3 | 4 | 9 592.1 | 106.6 |
| USA | 6 | 3 | 3 | 4 295.2 | 47.7 |
| Isle of Man | 4 | 0 | 4 | 605.6 | 6.7 |
| Switzerland | 5 | 3 | 2 | 3 427.3 | 42.5 |
| Hong Kong, China | 3 | 1 | 2 | 3 529.5 | 39.2 |
| Australia | 3 | 1 | 2 | 15 339.1 | 170.4 |
| Bermuda | 3 | 0 | 3 | 2 490.1 | 27.7 |
| Singapore | 5 | 3 | 2 | 2 991.51 | 33.26 |
| Comoros | 1 | 0 | 1 | 4 860.0 | 54.0 |
| France | 1 | 1 | 0 | 71.8 | 0.8 |
| Japan | 1 | 0 | 1 | 110.0 | 1.2 |
| Nigeria | 1 | 0 | 1 | 84 629.5 | 940.3 |
| Panama | 1 | 0 | 1 | 7 200.0 | 80.0 |
| **TOTAL** | **49** | **19** | **30** | **141627.72** | **1 577.86** |

## *Seeking other forms of international cooperation for AML/CFT purposes*

691. India has been proactive in seeking and providing informal international cooperation to a large extent, in keeping with its ML/TF risk profile. This is largely done by LEAs and the FIU-IND through regional and international organisations to which India is a member, such as INTERPOL and Egmont Group, and agency-to-agency cooperation for intelligence, operational coordination, and consultations prior to submitting formal requests.

### *Law Enforcement Authorities*

692. The ED uses its specially trained staff assigned to the Overseas Investigation Unit (OIU) to coordinate formal and informal international cooperation. The ED has also established direct contacts with counterparts to enhance informal relationships with foreign counterparts, including authorities from key strategic partners, such as the UAE, UK, United States and Singapore. The OIU conducts regular coordination meetings and discussions with these key partners to monitor the progress of requests and execute them. In total, over last three years ED has sent 45 requests for information on ML matters and received 23 responses, with 22 requests pending.

693. The Directorate of Revenue Intelligence (DRI) has signed 32 Customs Mutual Assistance Agreement (CMAA) with more than 60 countries. World Customs Organisation's network and gateways such as CEN (Customs Enforcement Network) are also used for exchange of information, and DRI uses a network of customs attachés located in various jurisdictions to support international cooperation, including in relation to drug trafficking investigations. The Income Tax Department has also signed various agreements with other countries to obtain information for the purposes of investigation under Indian Income tax laws. 160 such agreements have come in effect, assisting authorities in India to locate assets being hidden in offshore financial centres.

### Box 8.2. Trade-Based ML Network

Acting upon intelligence regarding potential diamond smuggling by a particular firm 'ABC' operating in a Special Economic Zone in Surat, DRI officers intercepted a vehicle and diamonds located within that vehicle. During the course of the investigation, four persons were arrested for smuggling under the Customs Act 1962. It was also revealed that the natural Cut & Polished Diamonds (CPD) imported from Hong Kong, China were actually synthetic diamonds which were then studded onto silver rings and exported back to Hong Kong, China and with a value more than 100 times what they were worth.

Investigations indicated the flow of money, primarily through banking channels through a web of dummy firms in India before being transferred via company ABC's account to overseas suppliers in Hong Kong, China under the pretext of payment towards import of diamonds. Gathered evidence also indicates that the mastermind of this trade-based money laundering was based in Hong Kong, China. Since October 2020, Company ABC had imported goods worth INR 10,305.9 million (EUR 114.5 million) and remitted INR 6 787.8 million (EUR 75.4 million) as payment. After the action by DRI, a further INR 3 518.1 million (EUR 39.1 million) was prevented from being transferred.

A reference under CMAA was made to Hong Kong Customs and Excise Department (HKCED) in September 2023 to exchange information and documents so that action could be initiated against the Hong Kong, China based suppliers, buyers and involved persons. DRI, under the existing bilateral international cooperation tools and network, had previously also reached out to HKCED to inquire into the existence of the suspected Hong Kong, China based firms which was used to locate the kingpins based in Hong Kong, China.

HKCED undertook an enforcement operation unearthing large-scale transnational money laundering syndicate that had laundered about EUR 60 million using the diamond trade. During the operation, HKCED raided eight premises across Hong Kong, China, arresting four persons suspected to be connected with the case and frozen a total of EUR 930 000 assets held by the alleged offenders.

694. The IPCU in the CBI hosts the National Central Bureau (NCB) for INTERPOL as well as the IPCC with specially trained staff to facilitate formal and informal international cooperation. The NIA has a dedicated unit under the Crime Division, specifically tasked with handling incoming and outgoing formal and informal international cooperation on TF matters. This unit is responsible for engagement with key stakeholders on TF matters, including Bangladesh, UAE and the United States.

695. The NIA and IB also utilise the NCB, in addition to a network of liaison officers and legal attachés, to support requests for assistance in TF and terrorism matters. This assists these authorities in intelligence gathering and operational activities to detect, investigate and disrupt TF and terrorism activities in India. During the period under review, IB sent 1 719 requests for assistance to foreign counterparts on CFT matters.

*FIU*

696. FIU-IND has been a member of the Egmont Group since 2007 and uses this network, in addition to the MOUs entered into with other counterpart FIUs, to seek and provide international cooperation. As detailed in Table 8.6 below, FIU IND has made 628 requests related to ML and 87 related to TF during the period under review. The quality of requests sent by FIU-IND, normally on behalf of LEAs, was generally good, with most countries providing feedback that they were able to action these requests from India. None of FIU-IND's requests have been refused and the only request withdrawn was not related to ML/TF.

### Table 8.6. Outgoing FIU requests

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (to Nov) | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests Sent | **263** | **477** | **405** | **517** | **351** | **224** | **2 237** |
| ML | 140 | 161 | 79 | 67 | 83 | 98 | 628 |
| TF | 16 | 15 | 20 | 8 | 20 | 8 | 87 |
| Requests executed | **259** | **437** | **375** | **482** | **301** | **150** | **2 004** |
| ML | 139 | 161 | 75 | 65 | 73 | 72 | 585 |
| TF | 16 | 15 | 20 | 8 | 20 | 6 | 85 |
| Pending | **4** | **39** | **30** | **35** | **50** | **74** | **232** |
| ML | 1 | 0 | 4 | 2 | 10 | 26 | 43 |
| TF | 0 | 0 | 0 | 0 | 0 | 2 | 2 |

### Box 8.3. International Cooperation via LEAs and FIU

Location of accused using INTERPOL Channel

Delhi Police initiated an investigation into a Mr. X, and several companies including M/s. Y Private Limited, for defrauding numerous unsuspecting investors through Ponzi schemes. Following this, the ED commenced a money laundering investigation into the directors and the company. It was revealed during the investigation that Mr. X, through his various companies, engaged in unauthorised businesses such as share trading, commodities trading, holiday packaging, and airfare ticketing, without the necessary legal sanctions and approvals required by law. He collected funds under the guise of a company named Z Airlines and misappropriated over INR 100 billion (EUR 1.1 billion) from innocent individuals.

During the investigation, it was discovered that Mr. X had travelled from India to Malaysia in 2019 and had not returned to India since then. To locate Mr. X in Malaysia, the Directorate requested assistance from NCB Kuala Lumpur through INTERPOL channels.

In response to the request, NCB Kuala Lumpur shared valuable information regarding Mr. X's travel details, confirming that he was indeed in Malaysia and had not left the country. The collaboration between the ED and NCB Kuala Lumpur facilitated the sharing of crucial information, helping establish the whereabouts of Mr. X and advancing the investigation into the Ponzi scheme fraud.

Use of EGMONT channels to support TF case (see case study in Box 4.4)

*Supervisory Cooperation*

697. Financial supervisors have sought cooperation from foreign counterparts, including through supervisory colleges, although this is largely in relation to fit and proper checks with no joint supervisory actions having been undertaken. Despite the lack of a clear lawful basis for international cooperation, the RBI has entered into international cooperation arrangements with a number of counterparts and has made five requests to overseas authorities for supervisory or other AML/CFT information, such as risk profiles and name screening, during the period under review. Requests to support fit and proper checks has also been sought by the RBI from foreign counterparts on 109 occasions during the period 2020-2023. Both SEBI and IRDAI have used the provisions contained within their relevant bilateral MOUs and MMOUs to seek this information as detailed in Table 8.7 below. No requests were made by IFSCA after assuming responsibility for the International Financial Centre in 2020. As noted in Chapter 6, IFSCA seeks input from other domestic supervisors (such as RBI and SEBI) on branches of Indian entities seeking to be licensed and foreign entities are required to provide a "no objection certificate" from their home regulator. Outside of this, IFSCA has not exchanged information with foreign supervisors during the period under review.

698. No international cooperation was sought by the FIU-IND as the AML/CFT supervisor for VASPs as of March 2023.

**Table 8.7. Outgoing Requests by Supervisors**

| | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 | TOTAL |
|---|---|---|---|---|---|---|
| Requests Sent | | | | | | |
| RBI | 0 | 0 | 10 | 32 | 67 | 109 |
| SEBI | 9 | 29 | 24 | 25 | 29 | 116 |
| IRDAI | 4 | 2 | 9 | 22 | 5 | 43 |
| Requests executed | | | | | | |
| RBI | 0 | 0 | 10 | 32 | 67 | 109 |
| SEBI | 9 | 29 | 24 | 25 | 25 | 105 |
| IRDAI | 4 | 2 | 9 | 22 | 5 | 42 |
| Pending | | | | | | |
| RBI | 0 | 0 | 0 | 0 | 0 | 0 |
| SEBI | 0 | 0 | 0 | 0 | 4 | 4 |
| IRDAI | 0 | 0 | 0 | 0 | 0 | 1 |

## *Providing other forms international cooperation for AML/CFT purposes*

699. India has also used its membership in key regional and international organisations, such as INTERPOL and Egmont Group, and agency-to-agency cooperation to provide international cooperation to foreign counterparts and non-counterparts.

### *Law enforcement authorities*

700. The ED receives informal requests for assistance in ML cases through channels such as Camden Asset Recovery Inter-Agency Network (CARIN), Asset Recovery Interagency Network Asia Pacific (ARIN-AP), as well as a number of bilateral arrangements. During the last 4 years, 106 requests related to ML were received by the ED and a significant majority of 83 requests (approximately 78%) have been already executed.

701. More than 10 000 requests are dealt with annually by NCB India (CBI) across a range of crime types, including ML and predicate offences. International conventions, multilateral and bilateral treaties and agreements, MMoUs and MoUs were regularly used for facilitating information exchanges by Indian LEAs, customs and tax authorities. The DRI received 345 foreign requests for investigative assistance under CMAAs and granted 190 of these during the period under review. There has been an increase in requests received since 2020 when transmission of diplomatic mail and post was impacted by the COVID pandemic.

8

### Box 8.4. Call Centre Fraud

Information was received from NCB Vienna through INTERPOL in August 2022 regarding an impersonation fraud carried out by an illegal call centre "XXX" operating from New Delhi, India, targeting victims in Austria, Australia, Germany and the UK. The alleged offenders extorted money by impersonating law enforcement officers and informing victims that their identities were stolen and drug offences had been committed in their names. Victims were defrauded of their money by way of bank transfers, crypto wallets, gift cards or voucher codes in order to clear their names.

Surveillance was launched and searches were conducted at several places associated with the crime in September 2022. Criminal prosecution has been launched in November 2022 against 4 accused persons under relevant sections of Indian Penal Code and Information Technology Act. 45.34 Bitcoins in six wallets (EUR 1 532 492)137, INR 7.5 million (EUR 83 772) in bank accounts and INR 3.5 million (EUR 39 093) in movable properties were seized during the investigation. Further analysis is ongoing with other crypto exchanges. The detection of crime and apprehension of offenders has led to the fraud being stopped in Austria, Germany and the UK. Information on victims has been shared via INTERPOL channels for further verification with Austria, Australia, Cyprus, Netherlands and Germany. Once victim details are verified, further action on seized assets can be initiated.

702. The NIA and IB regularly engage in informal international cooperation with counterparts in relation to TF. NIA has engaged in 86 police liaison officer (PLO)-to-PLO interactions and 27 spontaneous exchanges of intelligence and investigational details on TF cases over the period under review, and IB received 2 401 requests from foreign counterparts on CFT matters. Inputs from the FATF global network have raised no concerns with regard to India's approach to conducting joint investigations on behalf of or jointly with foreign counterparts. India is a signatory to both the Merida and Palermo Conventions and is able to engage in joint investigations under this legal basis.

*FIU*

703. FIU-IND has responded to almost all informal requests for information for the period under review and has not refused any requests, as detailed in Table 8.8 below. Of the 19 requests that are pending for 2023, nine relate to ML and two relate to TF. The FIU-IND also spontaneously disseminates information to other FIUs, with three out of the 12 spontaneous disseminations in the past five years related to ML.

[137] Based on the average closing price for Bitcoin in November 2023

**Table 8.8. Incoming FIU requests**

| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 (to Nov) | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests Received | **104** | **130** | **127** | **171** | **113** | **161** | **806** |
| ML | 24 | 27 | 27 | 52 | 31 | 72 | 233 |
| TF | 2 | 5 | 3 | 13 | 4 | 2 | 29 |
| Requests executed | **104** | **130** | **127** | **171** | **113** | **142** | **787** |
| ML | 24 | 27 | 27 | 52 | 31 | 63 | 224 |
| TF | 2 | 5 | 3 | 13 | 4 | 0 | 27 |

*Supervisors*

704. Financial supervisors have responded to limited requests from foreign counterparts but these largely related to fit and proper checks and due diligence requirements. For the period under review, RBI has received and responded to three requests from overseas authorities for supervisory or other AML/CFT information. Requests for fit and proper information has also been provided by the RBI to foreign counterparts on 199 occasions during the period 2018-2023. SEBI responded to 294 of 299 requests for information from foreign counterparts, in relation to fraud and misconduct investigations and fit and proper checks. IRDAI has received four requests for due diligence reports from foreign counterparts and responded to three of these, with the fourth request being withdrawn. No requests were received nor responded to by IFSCA during the period under review.

705. Feedback from countries indicated the information received was timely and of appropriate quality.

706. One request of international cooperation was received and responded to by the VASP supervisor during the period under review in relation to the VASP sector.

### *International exchange of basic and beneficial ownership information of legal persons and arrangements*

707. Competent authorities are providing basic and BO information on legal persons to a large extent. Basic and beneficial ownership information on legal persons is available publicly through the MCA website (although not always accessible outside of India), or via competent authorities in India. Authorities in India have provided specific details on how to access the information directly through the MCA website when responding to requests for basic and BO information. As per Table 8.9 below, competent authorities have provided BO information on several occasions during the period under review and feedback from foreign counterparts has been positive.

708. Competent authorities are able to access basic and BO information on legal arrangements, predominantly through FIU-IND and share with foreign counterparts. Competent authorities have shared this information with foreign counterparts, with the FIU-IND having shared information on legal arrangements on 10 occasions during the period under review.

### Table 8.9. Provision of basic and BO information

| | Requests Granted | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|---|
| FIU -IND | Requests related to legal persons | 25 | 41 | 38 | 52 | 38 |
| | Law enforcement requests (related to ML/TF only) | 14 | 23 | 23 | 16 | 15 |
| ED | Requests received to obtain basic ownership information for legal person | 0 | 2 | 8 | 9 | 6 |
| RBI[138] | Requests received for customer due diligence and BO information | 24 | 14 | 37 | 59 | 65 |
| SEBI[139] | Response to fit and proper requests on legal persons | 15 | 27 | 18 | 20 | 28 |
| CBDT[140] | Exchanges of information including BO on legal persons | 12 | 17 | 11 | 13 | 7 |

### Box 8.5. Sharing of BO information with foreign counterpart by FIU-IND

A request for information was received from the US FIU (FINCEN) in January 2022 regarding an individual under investigation for money laundering. This person was found to be associated with a specific company "A" which was alleged to be associated with accounts and legal persons operating in India. FINCEN sought assistance from FIU-IND suspicious transaction reports, bank account and BO details, as well as any other information available in the FIU-IND database.

Searches were carried out in the FIU-IND database and the MCA website and information on the basic, as well as the BO information, specifically name, address, e-mail id, passport number etc., were shared with the counterpart FIU. The information retrieved from the company registry established the BO and the same was shared with the counterpart FIU in June 2022 who responded positively.

[138] Statistics for RBI relate to financial years 2019-20 to 2022-23
[139] Statistics for SEBI relate to financial years 2018-19 to 2022-23
[140] Statistics for CBDT relate to financial years 2017-18 to 2021-22

## Overall conclusions on IO.2

India has provided and sought MLA and extradition to a large extent. The central authorities for MLA and extradition, MHA and MEA, prioritise requests sent and received related to ML/TF and the MHA has implemented new mechanisms which have significantly enhanced case management, coordination and the timeliness of responses to MLA requests, with the impact of these changes weighted significantly.

Indian authorities actively respond to formal international co-operation requests; however, a number of requests are pending full execution. Feedback on the quality of assistance provided is largely positive, although with recurring feedback from some counterparts indicating timeliness could be improved.

Feedback from some counterparts indicates the quality, specificity and coordination of outgoing requests could be improved. India is not identified as a strategic location for the laundering of foreign illicit proceeds and the volume of requests made is consistent with this profile. However Indian authorities are actively seeking MLA during the course of investigations, largely in keeping with their ML/TF risk profile.

Authorities have been proactive in seeking and providing informal international cooperation in keeping with India's ML/TF risk profile. ED and FIU-IND have sought and provided international cooperation with key partners both bilaterally and through regional organisations, and the NIA and IB also regularly engage with counterparts through other forms of international cooperation for CFT.

Most financial supervisors have sought and provided international cooperation, including information sharing through MOUs, although cooperation for most supervisors is limited in breadth and frequency. India effectively shares basic and beneficial ownership information of legal persons and arrangements, especially FIU-IND.

India is rated as having a substantial level of effectiveness for IO.2.

# TECHNICAL COMPLIANCE

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation published in 2010. This report is available from www.fatf-gafi.org.

## Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation, which was not assessed in the previous MER.

***Criterion 1.1 –*** India has completed a range of assessments to identify, assess and understand ML/TF risks. This includes national risk assessments (NRAs) of ML and TF first completed in 2011, with a second iteration in 2022. In addition, the following thematic or sectoral risk assessments (SRAs) on ML/TF risks including those related to Legal Persons and Arrangements (2023), Accountants, Lawyers and TCSPs (2022), Virtual Assets and Service Providers (2022) and the Postal sector (2023), as well as TF risk (2022) and NPO risk assessment for TF abuse (2023), Real Estate (2023), Assessment of Post Office (2023). There is also a detailed Risks, Trends and Methods Report (2019) that assesses ML risks related to the financial sector as well as TF risks.

***Criterion 1.2 –*** India has established a Joint Working Group (JWG) functioning under the aegis of the Inter-Ministerial Co-ordination Committee (IMCC), a statutory body under Section 72A of PMLA on AML/CFT.

The JWG is responsible for planning the NRA process, understanding the ML/TF risks, proposing measures for mitigating the risk, and examining the progress of the action plan produced to implement the mitigating measures. The JWG comprises of representatives from the Ministry of Finance, Ministry of Home Affairs, FIU-IND, ED, NIA, IB, CBDT, CBIC, CBI, RBI and other relevant stakeholders from the government sector.

***Criterion 1.3 –*** The IMCC as an organ of the government, is constituted under section 72A of the PMLA to coordinate the National Risk Assessment exercise to improve AML/CFT in India. An Office Memorandum (OM) dated 15th November 2018 released by the supervisor of FATF Cell (which is the secretariat for conducting risk assessments) requires the conduct of AML/CFT risk assessments periodically (once every three years). There have been two NRAs concluded since 2011 (2011 and 2022). Based on the OM, the next iteration of the NRA will be concluded in 2025.

***Criterion 1.4 –*** Although the NRA 2022 is a restricted document, the complete NRA has been disseminated to all competent authorities. An abridged version of NRA 2022, highlighting the results of the NRA exercise, has been shared with reporting entities that have access to the FINGATE portal via publication on the portal. Further, the Department of Revenue (DOR),

AML/CFT supervisors, and FIU-IND conduct frequent outreach in which conclusions in the NRA are communicated to the private sector (see IO.1).

Separate threat assessments of predicate offences and associated money laundering are also shared with all Competent Authorities. Key findings are included in publicly released annual reports (for example, the annual report of MHA, the annual report of DRI on smuggling, and annual report of NCB on illicit trade in narcotics) and are also shared through press releases. Similarly, abridged versions of SRAs have been shared with relevant reporting entities by email.

***Criterion 1.5 –*** India uses the understanding emanating out of the risk assessments it has conducted to apply a risk-based approach through the release of its National AML/CFT/CPF Policy Action Plan and Strategy Statement in 2023 ('Action Plan 2023'), supervision to oversee the implementation of the policies, deliberation on need for changes in law and rules, and setting up of operational level coordination bodies, if required.

The Action Plan 2023 mandates six broad focus areas to tackle ML and TF, which are prevention, detection, investigation, capacity building, cooperation, and outreach programmes. Amendments to the regulatory framework through the introduction of new laws, rules and guidance, have been made in response to identified threats and vulnerabilities for example in areas such as notification of VASPs as DNFBP, strengthening Beneficial Ownership rules etc.

Risks are also taken into account at the operational level through algorithm-based data mining tools that are used to identify actionable intelligence. The Enforcement Directorate (ED) allocates resources for ML investigations in a risk-based manner through a its Technical Circulars and Risk Assessment and Monitoring Committee (RAMC) (see IO.7). However, India did not demonstrate that its strategy for the allocation of resources such as staffing across the other authorities dealing with financial investigations is being informed by the risks identified.

***Criterion 1.6 –***

Real estate agents have reporting obligations under the PMLA, the AML/CFT/CPF Guidelines for Real Estate Agents issued in May 2023 provides for the exemption of real estate agents with a turnover of less than INR 2 million (EUR 22 222) from obligations under the PMLA. This is on the basis of low-risk exposure of real estate agents that who fall below the threshold. Various market factors and considerations of de-risking were considered into deriving this threshold in the 2023 Real Estate Sector Risk Assessment. The purpose of the exemption is not to impose an unduly burdensome AML/CFT regime on lower risk micro-business, to exempt transactions of a lower amount and to promote affordable housing. (see IO.1). While there has been some consideration of ML risks associated with the real estate sector such as cash purchases and benami transactions, India has not fully considered how the threats correspond with the exemption applied in the sector. No other exemptions on the basis of proven low ML/TF risk have been implemented.

a) n/a

***Criterion 1.7 –*** The PML Rules state that the regulator may prescribe enhanced measures to verify the client's identity taking into consideration the type of client, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risk involved (Rule 9(14)(i) PML Rules). The PMLA also requires additional steps to be taken to examine the client's ownership and financial position, including the source of funds (s12AA(1)(b) PMLA).

Enhanced measures applied by various regulators for products and services posing higher risks are detailed in guidelines issued by various regulators. Where higher risks are identified, this form of enhanced CDD process is applied in the opening and review of high risk accounts, non-face-to-face customer onboarding, accounts of foreign PEPs and professional intermediaries

(RBI's Master Direction on KYC), high risk clients and clients of special category (SEBI's Master Circular on AML/CFT ), for high risk patterns in insurance policies (IRDAI's Master Guidelines on AML/CFT), for high risk subscribers (PFRDA's Guidelines on AML/CFT) and for a list of high risk factors (IFSCA's Guidelines on AML/CFT). The PML Rules require reporting entities to incorporate relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. (Rule 9(13)(ii) PML Rules). This is further detailed to take into account sector specific considerations in the AML/CFT Guidelines of each sector.

***Criterion 1.8 –*** India has introduced products targeted at low-income population segments (e.g., Bank Mitra, Swabhiman campaign) and regulations/directions issued in respect of simplified due diligence measures are intended to promote financial inclusion or on identified low risk based on materiality.

Under the PML Rules, there are some exceptions to the requirement to verify the identity of clients where simplified measures are applied. These relate to small accounts (Rule 9(5) of the PML Rules) and small prepaid payment instruments (RBI's Master Direction on PPIs, para.9.1). See c.10.3)

These simplified measures are not permitted whenever there is a suspicion of money laundering or terrorist financing, where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment (Rule 9(14) PML Rules).

In addition, in the case of Foreign Portfolio Investors (FPIs), CDD documentation is tiered so that government and government-related foreign investors are exempted from submitting financial data, CDD documents for Authorised Signatures and BO. However, these have to be submitted upon demand by regulators and LEAs (RBI's Master Direction on KYC para 45).

***Criterion 1.9 –*** Guidelines on AML Standards and CFT /Obligations framed by Supervisors under the PMLA and Rules require Reporting Entities (REs) to carry out risk assessments regularly which must be consistent with any national risk assessment. Regulators of FIs and some DNFBPs have general powers to supervise, regulate and issue necessary directions. However, it has not been demonstrated that AML/CFT supervision is being conducted periodically based on ML/TF risk. No specific authority has been given powers and responsibilities for AML/CFT supervision for chartered accountants, notaries, lawyers and company secretaires. However, FIU-IND has issued guidelines for accountants, company secretaries and other TCSPs. SRBs are expected to monitor accountants, company secretaries and lawyers (including notaries). FIU-IND supervises TCSPs that are not company secretaries, or another FI or DNFBP. See analysis of R.26 and R.28 for more information.

***Criterion 1.10 –***

(a) – (d)

Every reporting entity is required to carry out a risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels. The risk assessment has to be documented; should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied; be kept up to date; and be available to competent authorities and self-regulating bodies (Rule 9(13) of the PML Rules).

Supervisors also require FIs and DNFBPs (except accountants and company secretaries and TCSPs) to take appropriate steps to identify, assess, and understand their ML/TF risks in accordance with the relevant sector specific AML/CFT Guidelines (RBI's Master Direction on KYC, SEBI's Master Circular on AML/CFT, IRDAI's Master Guidelines on AML/CFT, PFRDA's Guidelines on AML/CFT and IFSCA's Guidelines on AML/CFT).

***Criterion 1.11 –***

(a) – (c)

Regulators have issued circulars, directions or guidelines requiring financial institutions and DNFBPs to establish policies, controls, and procedures for managing the risks, implementing monitoring mechanisms and taking enhanced measures for mitigating the identified risks. Specific requirements for most FIs and DNFBPs are mandated by regulators in accordance with guidance (RBI's Master Direction on KYC, SEBI's Master Circular on AML/CFT, IRDAI's Master Guidelines on AML/CFT, PFRDA's Guidelines on AML/CFT and IFSCA's Guidelines on AML/CFT). This includes the requirement for senior management approval such as for transactions relating to foreign PEPs. Supervisors of professionals (accountants and company secretaries) and FIU-IND (other TCSPs) are in the process of developing risk-based supervision systems for compliance monitoring following their recent designation as AML/CFT supervisors.

***Criterion 1.12 –*** Simplified measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment (Explanation to Rule 9(14) of the PMI), 2005).

### *Weighting and Conclusion*

India has developed a generally comprehensive risk assessment process through its NRA and sectoral risk assessments, enabling it to identify, assess and understand ML and TF risks, communicate the findings to relevant stakeholders, and take mitigating action. There are some minor deficiencies, including a lack of clarity as to how allocation of resources is taking place in response to the NRA across all agencies, whether some provisions for exemptions and simplified measures are consistent with India's assessment of its ML/TF risks and the extent to risk-based supervision systems for compliance monitoring is developed for FIs and DNFBPs, particularly for more recently notified DNFBPs.

**Recommendation 1 is rated largely compliant.**

## Recommendation 2 - National Cooperation and Coordination

In its previous MER, India was largely compliant with R.31 as effectiveness of interagency co-ordination and co-operation had not yet been demonstrated.

***Criterion 2.1 –*** The National AML/CFT/CPF Policy Action Plan and Strategy Statement in 2023 ('Action Plan 2023') that addresses risks identified in the NRA, has been prepared as a high-level policy document on India's AML/CFT framework. The 2023 Strategy sets out six action plans focusing on prevention, detection, investigations, capacity building, cooperation, and outreach. The National AML/CFT Strategy Statement 2023-2028 Strategy is a five-year roadmap designed around the Action Plan 2023framework with short- and long-term actions.

Updated strategies for countering TF were also developed on the basis of the TF risk assessment reports prepared by an inter-ministerial working group, which had representation from competent authorities and the private sector. New strategies were developed and have been included in Chapter 8 of NRA 2022.

Updated strategies for countering TF were also developed on the basis of the TF risk assessment reports prepared by an inter-ministerial working group, which had representation from competent authorities and the private sector. New strategies were developed and have been included in Chapter 8 of NRA 2022.

***Criterion 2.2 –*** The IMCC was designated for AML/CFT policy coordination at the national level in 2019, under the chairpersonship of the Revenue Secretary (Notification dated 7th October 2019 for AML/CFT policy coordination). The mandate of IMCC is to ensure effective implementation of FATF standards, to draw, coordinate, monitor and review national AML/CFT policies and activities and their implementation, and to strengthen India's AML/CFT framework in line with FATF standards. Members of IMCC are Ministries of Home Affairs, External Affairs, Corporate Affairs, Departments of Economic Affairs, Financial Services, Posts, and the following organisations: CBDT, CBIC, CEIB, ED, CBI, FIU-IND, IB, NIA, NCB, SFIO, RBI, SEBI, and IRDAI.

The JWG under IMCC has been constituted with the Additional Secretary (Revenue), DOR as the Chairperson, to monitor and improve the effectiveness of India's AML/CFT regime. JWG comprises of representatives from MOF, MHA, FIU-IND, ED, CBI, NIA, IB, DRI, SFIO, NCB, CEIB, RBI, SEBI, IRDAI and other stakeholders (Office Memorandum dated 12th December 2019).

***Criterion 2.3 –*** IMCC and JWG, are the central bodies that act as mechanisms for the co-ordination and exchange of information to develop and implement AML/CFT policies. In addition, there are several other mechanisms in operation for national coordination and cooperation on AML/CFT at both the policy as well as operational level.

a) The CFT Cell, established by MHA, coordinates with domestic agencies on the development and implementation of CFT policies and operational activities.

b) Multi Agency Centre (MAC) is the key mechanism for sharing intelligence on national security measures, including TF.

c) The Special Investigative Team on Black Money is a Supreme Court monitored task force that assesses risks, makes policy recommendations and coordinates between LEAs and regulators in live investigations.

d) The Central Economic Intelligence Bureau (CEIB) coordinates information on financial crimes amongst LEAs and policy agencies through an information sharing protocol.

e) Fake Indian Currency Note Coordination Group (FCORD) coordinates on all CFT matters across different theatres of terrorist threats.

f) Financial Stability and Development Council – sub-committee considers policy issues such as amendments to PML Rules, use of Aadhar by entities and timely sharing of information by banks with LEAs.

g) FIU-IND Initiative for Partnership in AML/CFT coordinates strategic intelligence sharing on emerging trends with RBI and 46 reporting entities.

***Criterion 2.4 –***

A Multi-Agency Co-ordination Mechanism has been created with the objective of ensuring effective operational co-operation to combat the financing of the proliferation of weapons of mass destruction (F.No. 9-10/2023/CFT/FIU-IND dated 18th April 2023 /12A of WMD Act). This includes consultation on identification of names of individuals/entities for the purpose of proposing the same to UNSC for designation under resolutions 1718 and 2231.

India also has a SCOMET licensing regime which involves a multi-agency mechanism headed by the Director-General of Foreign Trade and comprises thirteen agencies that meet regularly over policy-making and operational implementation of the licensing of exports of dual-use goods and technology. The licensing process involves document verification as well as assessment and verification of end use relating to DPRK and Iran, and consideration of financial intelligence for these decisions.

The agencies included in the mechanism include, FIU-IND, RBI, SEBI, IRDAI, PFRDA, CBIC, CBDT, DRI, IB, NIA, Directorate General of Foreign Trade (DGFT, MEA), Disarmament and International Security Affairs (D&ISA, MEA), MCA, Centre-States Division of MHA and Union Territories Division of MHA.

***Criterion 2.5 –*** The rules governing data protection do not inhibit any of the AML/CFT requirements, as AML/CFT requirements in India override general data protection and privacy rules (Section 71 of the PMLA). There is no specific law in India for data localisation.

### *Weighting and Conclusion*

**Recommendation 2 is rated Compliant.**

## Recommendation 3 - Money laundering offence

In its previous MER, India was rated partially complaint with former R.1 and largely compliant with former R.2.

The main deficiencies related to:

a) A high monetary threshold condition for most ML predicates.

b) The ML provision did not cover the physical concealment of criminal proceeds.

c) The ML provision did not cover the sole knowing acquisition, possession and use of criminal proceeds.

d) Inadequate sanctions for legal persons committing the ML offence.

India has amended the Prevention of Money-Laundering Act on thirteen occasions between 2013 and 2019.

***Criterion 3.1 –*** The Republic of India ratified UN Convention against transnational organized crime on May 5, 2011, and UN Convention against illicit traffic in narcotic drugs and psychotropic substances on March 27, 1990.

Both conventions are enforced through The Prevention of Money-Laundering Act, 2002 (PMLA).

Criminal liability for the ML is established in PMLA "Offence of money-laundering". According to this section, ML is defined as a direct or indirect attempt to indulge as well as knowingly assisting or knowingly being as a party or actual involvement in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming.

The wording "*involvement in any process or activity connected with the proceeds of crime*" is very broad and covers the notions of the "*conversion*" and "*transfer*", which is also supported by the explanations provided in the technical circular ED/TECHNICAL CIRCULAR/HQ/13/2021[141] and the judgement of Honourable Supreme Court in case of *Vijay Madanlal Choudhary Vs. Union of India*.

The concept of "*projecting as untainted property"* and *"claiming as untainted property*" appears to be equivalent to the notion of "disguise". A mere act of projection or claim of illicit property as legitimate would be sufficient for the courts to establish the criminal intent.

[141] Dated 24.12.2021

***Criterion 3.2 –*** India uses the list approach for predicate offences. A list of predicate offences is contained in the relevant Schedule in the PMLA. As defined in section 2, scheduled offences include:

a) the offences specified under Part A of the Schedule;

b) offences specified under Part B of the Schedule if the total value involved in such offences is INR 10 million (approximatively EUR 112 000) or more (limited to smuggling only – see below);

c) Offences specified under Part C of the Schedule which captures the cross-border elements of offences.

A wide range of predicate offences in Part A of the Schedule apply to money laundering covering the designated categories of offences consistent with the FATF Standards, including any of the offences in Part A with 'cross-border implications,' which is specified in Part C. Part A includes a number of key sections of the Indian Penal Code (see below) as well as other criminal acts including (NPDS Act, Explosive Substances Act, The Arms Act, Unlawful Activities (Prevention) Act, The Wildlife (Protection) Act, The Immoral Traffic (Prevention) Act, Prevention of Corruption Act, among others).

The offences which are not covered directly in Part A or are covered through Part B or C are as follows. There are some minor gaps for Smuggling, Human Trafficking and Migrant Smuggling. Tax Offences are fully covered.

- *Smuggling*. Offences under the Customs Act, 1962, are in Part A (Evasion of Duty or prohibitions in Section 135 of the Customs Act) and partly covered in Part B (False declaration, false documents associated with a business transaction in Section 132 of the Customs Act). Part A covers all of the main activities as defined as smuggling by the World Customs Organisation, relating to goods or above the value of INR 10 million (EUR 112 000), evasion of duty above INR 5 million (EUR 56 000) or prohibited goods listed by the government. However, these thresholds are considered high in light of India's risk and context.
- *Human Trafficking and Migrant Smuggling*. The offences of slavery and trafficking in human beings in the IPC (sections 370, 371 and 374) are not predicate offences for ML, and instead India uses the Emigration Act, 1983, Immoral Traffic Prevention Act, 1956, The Bonded Labour Abolition Act, 1976, Child Labour (Prohibition and regulation) Act, 1986, Juvenile Justice (Care and Protection of Children) Act, 2015 to criminalise conduct associated with human trafficking and migrant smuggling (which are all predicates for ML under Part A). These offences do not capture all of the conduct that would be expected to be criminalised, specifically the trafficking of persons covering all aspects of recruitment, transportation, transfer, harbouring or receipt for the purposes of exploitation (human trafficking); and the procurement of the illegal entry into India for a material benefit whether directly or indirectly (migrant smuggling).
- *Tax Crimes*. Tax Crimes are considered predicate offences for ML as an act of fraud, cheating, conspiracy or criminal conspiracy against the State (IPC Art. 120B, 121A, and 420-424, with the Schedule Part A). In addition, wilful attempts to evade tax, penalties, or taxable interest are also predicate offences for ML for non-residents of India under Part C of the Schedule (Part C. with Section 51 of the Black Money [Undisclosed Foreign Income and Assets] and Imposition of Tax Act, 2015).

***Criterion 3.3 –*** India does not use a threshold approach to define predicate offences to ML or a combination of other approaches with a threshold approach.

***Criterion 3.4 –*** The term "proceeds of crime" has been defined in section 2(u) of the PMLA to mean any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property or where such property is taken or held outside the country, then the property equivalent in value held within the country or abroad.

The term "property" has also been defined widely in section 2(v) of the PMLA and means any property or assets of every description, whether corporeal or incorporeal, movable or immovable, tangible or intangible and includes deeds and instruments evidencing title to, or interest in, such property or assets, wherever located. It includes property of any kind used in the commission of an offence under the PMLA or any of the scheduled offences (Explanation to Sec 2(v) of PMLA).

***Criterion 3.5 –*** There are no rules in the PMLA that make it compulsory for a person to be convicted of a predicate offence in order to be sentenced for ML.

Section 44 of the PMLA states that the predicate offence and ML should be tried by the Special Court created for the area where the offence was committed, but the trial of both offences by the same court should not be construed as a joint trial.

***Criterion 3.6 –*** Under Part C of the Schedule, predicate offences include offences with cross-border implications. As specified in section 2, such an offence is defined as:

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 transfers in any manner 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.

***Criterion 3.7 –*** The offence of money laundering under Section 3 of the PMLA applies to any person covered by the Act. It does not provide any exception and includes the person who commit the predicate offence. Thus, a person can be charged simultaneously for the predicate offence and the offence of money laundering.

***Criterion 3.8 –*** The PLMA makes no restriction on the way in which the circumstances of the commission of ML can be established, nor on the inference of intent or knowledge of the commission of the offence. Moreover, in a number of cases the circumstances and intent to commit a crime can be established as presumptions, with the burden of rebuttal shifting to the defendant and the prosecution being relieved of the need to prove certain facts. For example, where money-laundering involves two or more inter-connected transactions and one or more such transactions is or are proved to be involved in money-laundering, then for the purposes of adjudication or confiscation or for the trial of the money-laundering offence, it shall unless otherwise proved to the satisfaction of the Adjudicating Authority or the Special Court, be presumed that the remaining transactions from part of such interconnected transactions (Section 23 of the PLMA). According to Section 24 of the PLMA, in any proceeding relating to proceeds of crime under the PLMA:

a) in the case of a person charged with the offence of money-laundering, the Authority or Court shall, unless the contrary is proved, presume that such proceeds of crime are involved in money-laundering; and

b) in the case of any other person the Authority or Court, may presume that such proceeds of crime are involved in money-laundering.

Thus, it is possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances.

***Criterion 3.9*** – Under Section 4 of the PMLA, a person who commits the offence of money laundering is liable to imprisonment for a term of not less than three years, but which may extend to seven years, and is also liable to a fine.

Where the predicate offence is an offence under the Narcotic Drugs and Psychotropic Substances Act, the maximum term of imprisonment for the crime of laundering the proceeds can be 10 years.

The range of penalties is comparable to other types of serious offences in India, and therefore are considered dissuasive on this basis.

There is no formal guidance for judges that would establish factors determining the severity of the penalty. However, the available case law suggests that higher sentences have been handed out in cases pertaining to TF-related activity, drug trafficking and corruption by highly placed public servants as compared to other offences. Therefore, the sanctions envisaged could be considered proportionate.

***Criterion 3.10*** – Section 70 of the PLMA contains provisions for holding legal persons and their managers liable.

A company which commits a contravention of any of the provisions of the PLMA or any rule, direction or order made thereunder, and every person who at the time of the contravention was in charge of the company and responsible to the company for the conduct of its business, shall be deemed to be guilty of contravention and shall be liable to be proceeded against and punished accordingly. An exception is made for the case where the person proves that the contravention occurred without his knowledge or that he exercised all due diligence to prevent such contravention. Both intentional commission of an offence and negligence are punishable offences.

A company is defined as any legal entity and includes a firm or other association of persons. A company may be held liable irrespective of whether the prosecution or conviction of any legal person is dependent on the prosecution or conviction of any natural person. Thus, sanctions can be applied independently of each other and do not preclude both natural and legal persons from being held liable for ML at the same time.

Section 4 of the PMLA provides two types of penalties in the form of imprisonment and fine, and legal persons can be sanctioned with a fine which is unlimited. A company can be wound up if the affairs of the company have been conducted in a fraudulent manner or the company was formed for fraudulent and unlawful purpose or the persons concerned in the formation or management of its affairs have been guilty of fraud, misfeasance or misconduct in connection therewith (Section 271 of the Companies Act). Any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud (Section 447 of the Companies Act). Therefore, the sanctions are deemed dissuasive or proportionate.

**Criterion 3.11** – Under Section 3 of the PLMA, the offence of ML covers a fairly wide range of acts involving direct participation or complicity, in particular

a) direct or indirect attempt to indulge in ML;

b) knowingly assisting in the commission of a crime;

c) knowingly taking part in a crime;

d) actual involvement in the crime.

It is apparent from the wording of the PLMA that participation in and association with the commission of money laundering, aiding and its attempt, facilitating and counselling the commission of money laundering are covered by the law.

Preparation to commit ML as an incomplete crime, as well as incitement as a form of complicity, is also punishable as demonstrated by the judgement of Honourable Supreme Court in case of *Vijay Madanlal Choudhary Vs. Union of India* (para 87(v)(a)).

### *Weighting and Conclusion*

India meets all the criteria with two exceptions. The designated categories of offences for trafficking in human beings and migrant smuggling where some elements of conduct are not covered, and the monetary threshold for offences under the Customs Act (which are equivalent to smuggling offences) is considered too high.

India has criminalised some key elements of the predicate offences above, and all of the other designated categories of offences that are higher risk offences in India. Therefore, these deficiencies are considered minor overall. There are no other shortcomings.

**Recommendation 3 is rated largely compliant.**

## Recommendation 4 - Confiscation and provisional measures

India was rated partially compliant with the former R.3 in its 2010 MER. The deficiencies related to a requirement for conviction for a scheduled predicate offences for confiscation, and weaknesses in the regime for confiscation of instrumentalities intended for use in terrorist acts. There were also no clear provisions to deal with assets in the event that the suspect was deceased.

**Criterion 4.1 –**

***Criterion 4.1(a)*** **–** India has legislative measures primarily under the PMLA to enable confiscation of property laundered, and supplemented by acts that include provisions for the criminalisation of offences [Fugitive Economic Offenders Act ('FEOA'), the Prevention of Corruption Act ('PCA'), and the Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act ('SAFEMA')]. Other acts provide additional provisions for confiscation.in relation to specific predicate offences [Customs Act, Narcotics Drugs and Psychotropic Substances (NDPS) Act and Arms Act]

The definition of property is set out in legislation and is consistent with the FATF definition [Section 2 (v) of the PMLA]. The process of attachment (seizure) of property, whether by criminal defendants or third parties, as property laundered and the subsequent steps for confiscation is also clearly set out [Sections 5 and 8 of the PMLA]. This also extends to property possessed, acquired, or used by a legal person [Sections 2(v), 2(s), 8(5) and 8(7) of the PMLA].

***Criterion 4.1(b)*** – India has legislative measures to enable the confiscation of proceeds and instrumentalities used in ML or predicate offences, with a minor scope gap in the coverage of some predicate offences. The definition of proceeds of crime extends to include property 'derived or obtained by the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence' (Section 2(u) of the PMLA). Section 2(v) of the PMLA also defines property in relation

to instrumentalities used in the commission of an offence. The footnoted explanations to these defined terms also extend to instrumentalities intended for use in ML or predicate offences.

***Criterion 4.1(c)*** - The Unlawful Activities (Prevention) Act (UAPA) 1967 is the primary legislation for the confiscation of proceeds of ***terrorism***. The proceeds of terrorism are defined to include proceeds from a terrorist act and properties used, or intended for use, for a terrorist act, or for an individual terrorist or organisation [Section 2(g) of the UAPA].

***Criterion 4.1(d)*** - Property of corresponding value can be confiscated under the PMLA. The definition of proceeds of crime extends to property of corresponding value (Section 2 (u) of PMLA). A similar definition of proceeds of crime exists in other legislation and competent authorities are able to confiscate property of corresponding value where an individual has fled the country (Section 2(k) and Section 5(1) of the ***FEOA)***. These confiscation powers are broader than what is required and also extend to other property held by an individual without requiring a strict link between the property and criminal conduct by virtue of the individual failing to appear before the courts (Section 8(7) of PMLA; Section 5(2) of FEOA). The confiscation of property of corresponding value extends to property linked to TF (Section 33(4) of UAPA).

**Criterion 4.2 -**

***Criterion 4.2 –a)*** **-** India has measures, including legislative measures, to enable competent authorities to identify, trace and evaluate property that is subject to confiscation. Broad powers are granted to officers of the Enforcement Directorate to identify, trace and evaluate property that may be subject to confiscation (Sections 16-24 of the PMLA). Similar powers are conferred to other law enforcement agencies (Section 6 of the FEOA, Section 43A of the UAPA and Sections 15-18 of SAFEMA). General investigative powers are provided for officers in relation to searching and identifying property that may be subject to confiscation in the course of an investigation (Sections 99-101 of the Criminal Procedure Code).

***Criterion 4.2 (b)*** **–** The PMLA contains provisions for the attachment of property as being the proceeds of crime. The ED is given the power to provisionally attach (seize) property asthe proceeds of crime on the basis of reasonable belief that the property is the proceeds of crime, and it is likely that those proceeds may be dealt with in such a way as to frustrate confiscation proceedings (Section 5(1) of the PMLA)]. Competent authorities are also given the powers to freeze (when it is not practical to seize) and seize property that is believed to be the proceeds of crime (Sections 17-21 of the PMLA). This can also be done *ex parte* (Sections 17-18 of the PMLA).

***Criterion 4.2 –c)*** - Section 9 of the PMLA provides the legislative basis for the Special Court, by way of an order, to declare void any actions that may prejudice the ability to freeze, seize or recover property that is subject to confiscation.

***Criterion 4.2 –d)*** - Various ***legislation*** provides powers for competent authorities to take investigative measures, including search and seizure and the production of information (see analysis in R.31).

***Criterion 4.3*** **-** India has laws and other measures to provide protection for the rights of bona fide third parties during ***investigation***, trial and post-trial. Protections are established for bona fide third parties, even in instances where notifications are not issued, to prove that property is not involved in ML (Sections 8(6)-(7) of the PMLA). Notices are also to be published in two newspapers, one in English language and one in vernacular language, regarding property confiscated in the local region (Ministry of Finance Notification No. 4/2016/P.12011/5/2015-S.O). This is a sufficient mechanism to notify bona fide third parties in order to establish claims to the property and to protect their rights.

***Criterion 4.4*** **–** The Central Government is able to appoint officers to perform the function of administrators of property frozen, seized or confiscated and to receive and manage this property

(Section 10 of the PMLA). Legislation also sets out the parameters for appointed administrators to dispose of property (Section 9 of the PMLA). India has mechanisms for the management and disposal of property such as cash, gold and jewellery (Rule 4 of the PMLA). Although not explicitly set out in the PMLA Rules, India has processes to manage incorporeal property or enterprises, including patents, businesses and virtual assets.

### *Weighting and Conclusion*

India meets all the criteria except there are minor gaps in the scope of predicate offences and an absence of explicit processes for the management of incorporeal property or enterprises.

**Recommendation 4 is rated largely compliant.**

## Recommendation 5 - Terrorist financing offence

India was rated partially compliant with the former SR.II in its 2010 MER. Criminalisation of TF was not in line with the TF Convention and did not cover the sole wilful act of financing individual terrorists and terrorist organisations. There were also few criminal convictions for TF. The UAPA, which is the principal legislation that criminalises terrorism and the financing of terrorism, has undergone amendments since 2010, including to the provisions relating to TF.

***Criterion 5.1 –*** India criminalises TF under the UAPA. The UAPA criminalises the provision or collection of funds, whether from a legitimate or illegitimate sources, with the intention that they are used in full or in part with by a terrorist organisation,[142] a terrorist gang[143] or by an individual terrorist to commit a terrorist act, whether or not the funds are ultimately used (Sections 15 and 17 UAPA). It is also clarified that raising or collecting or providing funds, in an any manner or for the benefit of, or, to an individual terrorist, terrorist gang or terrorist organisation for the purpose not specifically covered under section 15, shall also be construed as an offence. This is consistent with Article 2 of the TF Convention.

The definition of a terrorist act must have the intent of threatening, or likely threatening the unity, integrity, security, economic security of India, *or* the intent to or likely to strike terror to the people of India, any section of the people of India, or in any foreign country (Section 15(1)). The act should be to cause any one of the act listed in legislation, which includes causing death or injury to a person through the use of a list of dangerous substances (Section 15(1)(a)), using weapons, criminal force towards or causing the death of a public functionary[144] (Section 15(1)(b)), as well as detention, kidnapping, abduction or threatening to threat to kill or injure, *or* do any other act to compel the Government India, a foreign country, or an international or inter-governmental organisation or any other person from abstaining from acting or encouraging them to act in a particular way (Section 15(1)(c)). The definition of a terrorist act under the UAPA also covers acts which constitutes an offence within the scope of, and as defined by, one of the treaties listed in the Annex of the TF Convention (Section 15(2)).

[142] Defined in Section 2 of the UAPA as an organisation listed in first Schedule or an organisation operating under the name as an organisation listed.

[143] Defined in Section 2 of the UAPA as any association, other than a terrorist organisation, whether systematic or otherwise, which is concerned with, or involved in, a terrorist act.

[144] Meaning a member of the constitutional authorities or any other functionary notified in the Official Gazette by the Central Gazette by the Government as a public functionary, such as a minister, member of the legislative assembly, or a Chairman Vice Chairman or Managing Director of a board of directors engaged of a public body or company or corporation controlled by the Government of India.

These acts criminalise a terrorist act described in part 1(b) of Article 2 of the TF Convention, sufficient to satisfy criterion 5.1, while also covering acts that are beyond the scope of the Convention.[145]

***Criterion 5.2 –*** The UAPA criminalises the act of directly or indirectly, raising, providing or collecting funds, whether from a legitimate or illegitimate source, from any person/s or attempting to provide to, or knowing that such funds are likely to be used, in full or in part by such person/s or by a terrorist organisation or by a terrorist group or by an individual terrorist to commit a terrorist act, notwithstanding whether such funds were actually used or not for commission of such act. (Section 17 of the UAPA). The explanation to the provision in the legislation confirms that raising, collecting or providing funds, in any manner for the benefit of, or to an individual terrorist, terrorist gang or terrorist organisation for the purpose not specifically covered under section 15 (scope of terrorist act), shall also be construed as a TF offence and thus covers even in the absence of a link to a specific terrorist act/s.

***Criterion 5.2bis –*** While the financing of travel for the purpose of committing a terrorist act or providing or receiving terrorist training is not specifically covered by the UAPA, several provisions cover synonymous activity including conspiracy, organising terrorist camps and recruitment (Sections 15 to 20 of the UAPA). Returning foreign terrorist fighters have faced these charges under the UAPA.

***Criterion 5.3 –*** The UAPA covers raising or collecting funds "whether from a legitimate or illegitimate source." The reference is confined to funds rather than funds or other assets. (Section 17 of the UAPA). However, India has referred to MHA circular No. 14012/06/2022/CFT issued on 22 November 2023, attesting that the interpretation of funds in the legislation is interpreted to mean both funds and assets. This is supported by judicial cognisance of the legal position. In several cases, the courts have accepted that a prima facie case had been made out where the accused was charged for raising non-financial assets such as raw material to make weapons, mobile phones etc.

***Criterion 5.4 –*** The TF offence applies to funds that are provided to, raised or collected for a terrorist or terrorist organisation, whether such funds were actually used or not, to carry out or attempt a terrorist act even in the absence of a link to a specific terrorist act. (Section 17 of the UAPA)

***Criterion 5.5 –*** The intent requirement under the UAPA is "knowing that such funds are likely to be used." Although the provision is silent with respect to the proof required to establish knowledge, the general evidentiary provisions under the Indian Evidence Act (Section 106 and 114 of the Indian Evidence Act) allow knowledge required to prove the offence to be inferred from objective factual circumstances. This has been understood and applied in criminal prosecution.

[145] For example under section 15(1) of the UAPA, a terrorist act also includes any act with the intent to threaten or likely to threaten the "economic security" of India, by a list of harmful means which includes "by any other means of whatever nature", acts that disrupt "any supplies or services essential to the life of the community in India or in any foreign country, acts that "cause damage to the monetary stability of India by way of production or smuggling or circulation of high quality counterfeit India paper currency, coin or of any other material".
Please also see comments letter to the FATF dated 31 October 2023 from the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the situation of human rights defenders which can be found here

***Criterion 5.6 –*** Criminal sanctions are proportionate and dissuasive for natural persons convicted of terrorist financing. The prescribed punishment for raising funds for a terrorist act is imprisonment for not less than five years and which can extend to life imprisonment and a fine (sec 17 UAPA); for raising funds for a terrorist organisation is imprisonment of up to fourteen years and/or a fine (section 40 UAPA); and for support to a terrorist organisation is a term of imprisonment of up to ten years and/or a fine (section 39 UAPA). Where India's legislation does not prescribe the amount of fine, this is left to the Courts based on judicial sentencing principles and precedents.

***Criterion 5.7 –*** Section 22 A and C of the UAPA read with the definition of 'person' under section 2 UAPA suggests that companies can be held criminally liable for offences committed under the UAPA and this has been confirmed by case law. However, other than being able to wind up the company under the Companies Act liabilities under the Income Tax Act, the UAPA does not clearly indicate what criminal sanctions apply to the legal entity itself and thus it is not possible to assess whether sanctions are proportionate and dissuasive. The punishment prescribed under the UAPA applies to the person who was "responsible for the conduct of business" (s22C UAPA). Although TF charges have been preferred against legal persons, there have not been any convictions and sentences passed so far.

***Criterion 5.8 –***

a) attempt to commit the TF offence

The general TF offence under the UAPA includes an attempt to commit the TF offence (section 17 UAPA)

b) participate as an accomplice in a TF offence or attempted offence

The explanation to section 17 UAPA clarified that the general TF offence under the UAPA includes participation (section 17 UAPA).

c) organise or direct others to commit a TF offence or attempted offence

The explanation to section 17 UAPA clarified that the general TF offence under the UAPA includes organising and directing (section 17 UAPA)

d) contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose.

The facilitation of the commission of a terrorist act or an act preparatory to the commission of a terrorist act is criminalised under the UAPA (section 18 UAPA). In addition, a person who provides support, including financial support, to a terrorist organisation with the intent to further its activity commits an offence under the UAPA (section 39 UAPA).

***Criterion 5.9 –*** TF offences are designated as predicate offences for ML under section 4 of the PMLA. The Scheduled offences (predicate offences) under the PMLA includes a list of TF offences under the UAPA in paragraph 4 which covers TF offences (Section 17 and 40 UAPA).

***Criterion 5.10 –*** TF offences apply regardless of whether the person commits the act in the same country or a different country to the one in which the terrorist or terrorist organisation is located or the terrorist act occurs/will occur. The 'Terrorist act' has been defined in Section 15 to include acts committed outside India. Accordingly, Section 17 i.e., punishment for raising funds for 'terrorist act' covers financing of 'terrorist acts' committed in India as well as in foreign country. In addition, any individual who commits TF outside of India associated with an act of terrorism in India shall be subject to the provisions the UAPA as though the offence had been committed within India (Section 1(4)).

### *Weighting and Conclusion*

The UAPA provisions do not indicate what criminal sanctions apply for TF to the legal entity itself. The punishment prescribed under the UAPA applies to the person who was "responsible for the conduct of business". While there are several cases involving the involvement of legal persons in TF, the deficiency is minor considering most are shell companies used to move funds, and can be dealt with through civil and administrative actions under the Companies Act and Income Tax Act.

**Recommendation 5 is rated largely compliant.**

## Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its previous MER, India was rated as largely compliant for SR.III. Outside the financial sector, there was no indication of effective implementation of guidelines issued and no monitoring to ensure compliance with the freezing mechanism. There were also no procedures in place to allow affected persons to have access to funds for basic expenses.

***Criterion 6.1 –***

a) The MHA is the competent authority that proposes individuals or organisations for listing under the UNSCR 1267 (1999), 1988 (2011) and 1989 (OM No. 14012/06/2022/CFT-81).

b) The mechanism for identifying targets for designation based on the designation criteria set out in UNSCRs 1267 and 1988 Committee is set out in section 35 of the Unlawful Activities (Prevention) Act 1967 read with OM No. 14012/06/2022/CFT-82.
Under the mechanism for this, input is received from the LEAs, intelligence agencies and other security agencies. The MHA coordinates this via the Multi Agency Centre (MAC) that meets regularly to discuss the merits of proposals for each target or designation developed. MHA then reviews the recommendations/inputs from the MAC and if it believes that the individual or organisation fits the designation criteria under section 35 of the UAPA, the designation is notified in the official gazette of India and added to the Schedule/s in the UAPA.

c) The application of the criteria to propose designation is based on reasonable grounds based on the criteria set out in the UAPA, and is not contingent upon the existence of a criminal-proceeding against the individual or organisation (OM No. 14012/06/2022/CFT-81/ OM No. 14012/06/2022/CFT-82).

d) Designation proposals from the Government of India is forwarded to the Ministry of External Affairs, Government of India for submission to the concerned Committee of the UNSCR in the prescribed format which follows the UN procedure (OM No. 14012/06/2022/CFT-81).

e) The MEA provides as much relevant information as possible on the proposed name in the format prescribed by the concerned committee of the UNSCR which contains as much detail as possible on the basis for the listing consistent with the UNSCR form which includes identity, key identifying information, travel documents, aliases, physical description, as well a statement of the case, basis of listing and whether India's status as the designating state may be made known (OM No. 14012/06/2022/CFT-81).

***Criterion 6.2 –***

a) The MHA is the competent authority for designation of targets identified on India's own motion and for making designations pursuant to requests from other countries under UNSCR 1373 (OM No. 14012/06/2022/CFT-82).

b) The mechanism for identifying targets for designation based on the designation criteria in UNSCR 1373 is set out in section 35 Unlawful Activities (Prevention) Act 1967 read with OM No. 14012/06/2022/CFT-82.

Under this mechanism, input is received from LEAs, intelligence agencies and other security agencies. The MHA coordinates via the MAC that meets regularly to discuss the merits of proposals for each target or designation developed. The MHA then reviews the input from the MAC and if it believes that the individual or organisation fits the designation criteria under section 35 of the UAPA, the designation is notified in the official gazette of India. Where these are based on the designation criteria set out in the UNSCR 1373, the proposals to designate such individuals or organisations are sent by the MHA to the MEA for forwarding to other jurisdictions for designation (para 5 of the OM No. 14012/06/2022/CFT-82).

c) To give effect to the requests of foreign countries under the UNSCR 1373, the Ministry of External Affairs examines requests and forwards them electronically *without delay*, with their comments, to the MHA. As MHA examines the request *without delay*, so as to be satisfied that the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organisation (Paragraph 8 of the Order 14014/01/2019/CFT).Without delay is defined to be "*on the same business day but no later than 24 hours*" and thus corresponds to the requirement to make a prompt determination.

d) Designations pursuant to UNSCR 1373 are based on the standard of proof of reasonable grounds that the individual or organisation is believed to be involved in terrorism and is not contingent upon the existence of a criminal proceeding against the individual or organisation (Section 35 of the UAPA with OM No. 14012/06/2022/CFT-82).

e) When submitting proposals under the UNSCR 1373 to other countries, MHA is required to provide as much relevant information supporting the designation, as possible (Paragraph 5 of the OM No. 14012/06/2022/CFT-82). This OM also prescribes a standard format for submitting requests to other countries under UNSCR 1373 with all the relevant details.

***Criterion 6.3 –***

a) The investigating authority has the legal authority to obtain information, in relation to offences under the UAPA, or on points or matters that will be useful for or relevant to the purposes of the UAPA terrorism and terrorist financing offences set out the UAPA (Section 43F of the UAPA

b) MHA has the power to issue *ex-parte* orders for designating an individual or organisation under the UAPA (OM No. 14012/06/2022/CFT-82).

***Criterion 6.4 –*** Section 51A of the UAPA gives the Central Government the powers 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 Order (Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended), or any other person engaged in or suspected to be engaged in terrorism. The

procedures for implementing TFS related to terrorism are proscribed in the OM No. 14014/01/2019/CFT, dated 2nd February 2021 as amended ("OM").

Whenever an update is made to the UNSC list, the MEA electronically forwards the changes without delay to the designated nodal officers in the MCA, CBIC, Financial Regulators, FIU–IND, CTCR Division and Foreigners Division in MHA. (Paragraph 4, OM No. 14014/01/2019/CFT). The regulatory agencies then forward the list of designated persons without delay to the regulated entities and MHA shall do the same to their state nodal officers, immigration authorities and security agencies. The entities that are covered in the OM include banks, stock exchanges and depository institutions, intermediaries regulated by SEBI, insurance companies, registrars performing the work of registration of immovable properties and DNFBPs (including casinos, real estate agents, DPMS, lawyers, notaries, accountants, company service providers and societies/firms), NPOs, chartered accountants and the Registry of Companies.

The same process is followed for designations by MHA under UNSCR 1373 except that this is communicated to the nodal officers by MHA rather than MEA.

The list of designated persons under UNSCR 1267 and 1988 is published on the MEA website and the list under UNSCR 1373 is published on the MHA website. Updates to the list are also forwarded to the reporting entities registered with FIU-IND through the publication of the list on FINGATE.

FIs, DNFBPs and VASPs are also required to maintain updated designated list in electronic form and screen regularly to verify whether designated individuals or entities are holding any funds, financial assets or economic resources or related services through their respective guidelines (Master Direction issued by RBI, Circulars issued by SEBI and PFRDA, Master Guidelines issued by IRDAI, AML/CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets, SOPs by CBIC for REAs and DPMS).

Where there is a match, the OM places obligations on these entities to inform their designated nodal officer as well as MHA without delay, as well as not to deal with the asset. MHA will conduct enquiries to verify the information and if it confirms a match, MHA will issue an order under section 51A of the UAPA to freeze the asset.

A corrigendum issued on 29th August 2023, adds a more explicit obligation for any natural and legal persons person holding the asset of a designated entity to "without delay and without prior notice" freeze by informing the nearest police station. The police will then follow same procedure in the OM No.14014/01/2019/CFT that should lead to a freezing order under section 51A of the UAPA.

The OM requires that the communication to the state nodal officers is conducted "without delay", that any matches are communicated to the designated nodal officer as well as MHA "without delay" and that MHA should conduct verification and issue an order under section 51A of the UAPA to freeze the asset "without delay". On 20th October 2023 India issued a further OM clarifying that TFS designations under UAPA 51A are "publicly available on the website of the FIU-India for wider access by all natural and legal persons" and in order that "sanctions are imposed 'without delay' as required in different International Conventions", "[a]s per the established conventions and practice it is clarified that 'without delay' in the context of sanctions related to Terrorism and Terror Financing as well as Proliferation Financing means preferably on the same business day but not later than 24 hours in any case". The intent of the 24-hour clarification is to formalise the entire sanctions process from UN changes to the communication by the MEA to the reporting entities through the Regulators, FIU Website and FINGATE portal, to the identification. This formalisation of the existing process can be read as applying to the entire process as intended, but it also introduces the possibility that reporting entities have an additional 24 hours to identify and freeze. In practice, both among the authorities and the FIs

interviewed the commonly accepted definition was immediately and not more than 24 hours after the UN listing and communication by the MEA through regulators to the FIs and VASPs. For DNFBPs interviewed, some were under the impression that they had a full 24 hours after the MEA communication.

***Criterion 6.5 –***

a) Under the UAPA, a person is defined broadly and covers legal and natural persons. The electronic communication by the MEA of changes to the UN lists causes the names of designated individuals and entities to be inserted in the Schedule of the UAPA. The legal obligation for all natural and legal persons to freeze is clarified in the corrigendum of the OM dated 29 August 2023 which inserted para. 7(ix) to be read with paragraphs 6.2 to 6.6 of the OM which reads that "(A)ny person, either directly or indirectly, holding funds or other assets of designated individuals or entities, shall, without delay and without prior notice, cause to freeze any transaction in relation to such funds and assets by immediately communicating this to the nearest Police Station (para 7(ix) OM No.14014/01/2019/CFT as amended on 29th August 2023). As described in 6.4, natural and legal persons were reminded to check the FIU website for changes to the UN list and to implement the sanctions process without delay clarified to mean "preferably on the same business day but not later than 24 hours (OM nos. 12011/14/2022-ES Cell DOR dated 20th October 2023). For FIs and DNFBPs, the OM has explicit prohibitions for the dealing of the funds (para 5(iv), 6(2), 7 (i)(a), 7(ii), 7(viii) OM No.14014/01/2019/CFT).

Regulatory sanctions are available under the respective regulations for FIs for breaches of the OMs and TFS obligations under the regulations. This is less clear with DNFBPs as their regulator (CBIC) does not have inherent sanctioning powers for TFS. India referred to general powers to penalise reporting entities under s13 of the PMLA if they fail to fulfil their sanctions obligations. For natural and legal persons, India has referenced the s3 of the UAPA on the enforceability of the 6.5(a) freeze obligations i.e., "every person shall be liable to punishment under this Act for every act or *omission* contrary to the provisions thereof, of which he is held guilty in India" read with the explanation in Section 17(c) of the UAPA (penalty for TF offences) which states that "raising or collecting or providing funds, in any manner for the benefit of, or, to an individual terrorist, terrorist gang, or terrorist organization for the purpose not specifically covered under section 15 shall also be construed as an offense." The authorities contend that based on case law, section 17 places the burden of knowledge on the defence (*Redaul Hussain Khan v. NIA* [2013(1) GLT 880]). However, as the knowledge requirement for a TF offence and an offence for breaches of freezing obligations under a TFS framework is not the same, s17 UAPA would not always be the appropriate sanction for pure breaches of the TFS framework. (see also R.35)

b) The obligation to freeze under the TFS framework covers designated persons and entities and is not tied to a particular terrorist act, plot or threat (c.6.5(b)(i)). It covers "funds and financial assets or economic resources held by, on behalf of or at the direction of" the designated persons or entities (c.6.5(b)(iv)) (Section 51A of the UAPA read with Order No. 14014/01/2019/CFT). In addition, the corrigendum covers funds and other assets of designated entities held "either directly or indirectly" (c.6.5(b)(ii)). (Section 51A of the UAPA read with Order No. 14014/01/2019/CFT including corrigendum 29th August 2023).

To demonstrate the applicability of wholly or jointly owned or controlled (c.6.5(b)(ii)), India provided a case where the central government under Section 51 has been able to attach property of a designated terrorists with a portion of ownership in immovable property. To demonstrate

assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities (c.6.5(b)(iii)), in the same case as agricultural produce from those lands were also attached. While the latter two criteria are not explicitly found in the legislation, case law demonstrates that the scope is interpreted broadly as intended in c.6.5.

c) There is a prohibition for any individual or entity from making funds, financial assets or economic resources or related services available for the benefit of designated entities. Section 51A(b) of the UAPA refers to designated individuals or entities listed in the Schedule to the Order. Para 4 (d) and (e) of this Order prohibits any individual or entity from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of individuals or entities listed in the Schedule and persons or entities acting on behalf of or at the direction of such individuals or entities". Similar to c.6.5(b), case law can be relied on to interpret the scope broadly.

d) There is a communication mechanism between the regulators and REs regarding their obligation if they find a match to designated individuals or entities (see c.6.4 and OM No. 14014/01/2019/CFT dated 2nd February 2021). In addition, communication of designations to FIs and DNFBPs registered under FIU-IND's FINGATE Portal also takes place via the portal. Regulators have issued guidelines in accordance with the OM to the entities that they supervise. There is no similar guidance for all natural and legal persons.

e) FIs and DNFBPs are required to report to their nodal officers as well as MHA any assets held by designated entities, whether frozen or not. (Paragraphs 5.1, 7 (iv) Order No. 14014/01/2019/CFT; paragraph 7(1)(a) corrigendum to Order No. 14014/01/2019/CFT as amended in August 2023).

f) Under the UAPA, no order of forfeiture shall be made against a bona fide transferee of proceeds without knowing that they represent proceeds of terrorism (section 27(2) UAPA). Only government officers including government competent authorities are protected from prosecution or legal proceedings for acts conducted in good faith in pursuance of the UAPA (section 49 UAPA). However, there is no explicit prevention of prosecution or legal proceedings of other persons who in good faith, take action in relation to assets when implementing the obligations under the UAPA. India explained that the provision covers government authorities and all the persons acting under the authority of law/order of a government officer- which essentially translates to the extension of protection to every person acting in good faith- under the Act and the Orders under the Act issued by a Government authority based on a plain reading of the statue and related definitions in the UAPA. There is no case law on point to test this interpretation.

***Criterion 6.6 –***

a) The OM No. 14012/06/2022/CFT-81 that is available on the MHA website, provides the link in paragraph three to the de-listing procedure available on the UN website. It also states that for the submission of any delisting request by India, the procedure outlined in the UNSCR1267 (1999), 1988 (2011) and 1989 (2011) Committee's guidelines are to be followed.

b) The MHA is the legal authority to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373, that no longer

meet the criteria for designation (section 36 UAPA read together with the 'Procedure for Admission and Disposal of Application Rule 2004') and has the legal authority to unfreeze such funds. (Paragraph 11 of the Order No. 14014/01/2019/CFT as amended by the Order No. 14012/06/2022/CFI3).

c) The UAPA, lays down the procedure for a review of the designation by a Review Committee which is chaired by a serving or retired judge of the High Court. The review committee must pass an order within one month of the receipt of the application by an entity or individual (Section 36 of the UAPA).

The decision of the Review Committee can be reviewed by the High Court. The applicant can file a petition in a High Court in India under article 226 of the Indian Constitution, which provides the power to issue writs, including writs in the form of *habeas corpus*, *mandamus*, prohibition, *quo warranto*, or *certiorari*, to any person or authority, including the government.

d) Paragraph 4 in OM No. 14012/06/2022/CFT-81 states that submission of any delisting request by India, procedures as outlined in the UNSCR1267 (1999), 1988 (2011) and 1989 (2011) Committee's guidelines are to be followed. Also, the FAQs regarding designation under UNSCR 1267/1988 on the website of the MHA makes the designated persons and entities aware of the procedures available for review of designations, including the Focal Point mechanism established under UNI 1730.

e) Paragraph 4 in OM No.14012/06/2022/CFT-81 states that for the submission of any delisting request by India, the procedures outlined in UNSCR1267 (1999), 1988 (2011) and the 1989 (2011) Committee's guidelines are to be followed. The website of MHA, in its FAQs section, also contains information about the United Nations office of the Ombudsperson which can be accessed by the designated persons and entities.

f) Para 11 of the order No 14014/01/2019/CFT lays down the procedure for unfreezing the funds or other assets of persons or entities with the same or similar name as designated persons or entities, if it has evidence to prove that funds have been inadvertently affected by a freezing mechanism (i.e., false positives). The details have also been included in the FAQs maintained on the MHA's website.

g) Para 4 and 11A of the order No 14014/01/2019/CFT as amended by Order No.14012/06/2022/CFT-83 lays down a mechanism for communicating de-listings and unfreezing measures to FIs and DNFBPs. It also provides guidance to FIs DNFBPs and other persons or entities regarding the action to be undertaken by them in order to release the funds upon receipt of a de-listing order.

***Criterion 6.7 –***

India authorises basic and extraordinary expenses by exempting freezing procedures under the Order No.14014/01/2019/CFT, for funds and other financial assets or economic resources that have been determined by the designated Central Nodal Officer of the UAPA (paragraph 10). This is in accordance with UNSCR 1492. (Para 10.3 of the Order No 14014/01/2019/CFT as amended by Order No 14012/01/2019-CFT-83 provides the procedure for making such requests.)

### *Weighting and Conclusion*

There are minor shortcomings in India's TF-TFS framework, particularly relating to the lack of clarity in the language of the OM regarding the implementation of TFA without delay.

**Recommendation 6 is rated largely compliant.**

## Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation, which was not assessed in the previous MER.

***Criterion 7.1 –***

The financing of activities of any order issued under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005 (WMD Act) is prohibited (Section 12A of the WMD Act). The prohibition relating to the specific UNSCRs relevant to the criterion is imported through orders issued by the Ministry of External Affairs as the competent authority, after these are adopted by the UNSC, which based on the WMD Act, is when the financing prohibition applies. The prohibition is implemented in accordance with Order F.No. P-12011/14/2022-ES Cell-DOR dated 1st September 2023 was issued by the DOR, MOF ("DOR WMD").

The MEA will electronically communicate, without delay, the changes made in the list of designated individuals and entities to the Central Nodal Officer (CNO) who is the FIU-IND, and to nodal officers, which include MHA, MCA and regulators as defined under the PMLA Rules. OM nos. 12011/14/2022-ES Cell DOR dated 20th October 2023 clarifies this to mean "preferably on the same business day but not later than 24 hours in any case". Based on the information, the CNO updates and maintains the designated list on the portal of FIU-IND (which is available to registered reporting entities) as well as the FIU website (which is public-facing). The legal obligation to freeze these assets arises at this stage (i.e., when FIU-IND updates its list on its portal). (s5.1 DOR WMD).

India also imposes ongoing screening obligations on FIs and VSAPs through their respective guidelines (Master Direction issued by RBI, Circulars issued by SEBI and PFRDA, Master Guidelines issued by IRDAI, AML/CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets) which require entities to regularly screen new and existing customers against UNSC list relating to proliferation financing.

In addition, regulators, who are nodal officers, are required to share updates to the lists, with their respective reporting entities. The nodal officer from MHA is required to share the same with immigration and security authorities. The DOR WMD requires that these transmissions take place without delay. The DOR WMD mandates Financial Institutions and DNFBPs to verify if the particulars of designated individuals and entities and in case of a match, stop transactions, provide information to the CNO as well as to file an STR if a match is found. Upon verification, the authorities will obtain an order relating to the financing and freezing the immovable property of the designated entity. The DOR WMD requires all natural and legal persons holding any funds or assets of designated persons or entities to freeze the funds and assets and transactions without delay and without prior notice. (Paragraph 5.1 of the DOR WMD).

***Criterion 7.2 –***

a) The DOR WMD requires all natural and legal persons holding any funds or assets of designated persons or entities to freeze the funds and assets and transactions without delay and without prior notice. (Paragraph 5.1 of the DOR WMD). Punishment for the contravention of the order is imprisonment of up to one year or fine or both (s19 WMD Act).

b) The obligation under the DOR WMD extends to all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation (s.7.2(b)(i)); those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities(s.7.2(b)(ii)), as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities(s.7.2(b)(iv)) and funds or assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities (c.7.2(b)(iii)). (Paragraph 5.1 of the DOR WMD )

c) There is a legal prohibition on all persons not to finance activity prohibited under the WMD Act, including the DOR WMD as well as related to the designated list of individuals and entities which in its implementation under the DOR WMD prevents funds or assets from being made available to or for the benefit of designated persons or entities, unless an exemption has been granted under the DOR WMD. (Paragraph 12A of the WMD Act; Paragraph 5.2 of the DOR WMD). "(P)erson" shall include any company or association or body of individuals, whether incorporated or not (General Clauses Act 1977).

d) The MEA is required to electronically communicate without delay, the changes made in the UNSC Sanctions List under the relevant UNSC resolutions related to WMD proliferation, to the CNO. MEA and the CNO will also communicate this to other Nodal Officers, which include regulators. (see also c.7.1) Updates to the list are also communicated to reporting entities registered under the FIU-IND through the FINNET, through which the updated designated list as updated by the FIU-IND is maintained. Regulators are required to communicate the updated designated list, without delay to their REs (Paragraph 2 DOR WMD)

The DOR WMD Order provides procedural guidance to financial institutions, registrars of properties as well as DNFBPs that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms (Paragraphs 3 to 5 of the DOR WMD Order).

e) FIs and DNFBPs are required to report to the State Nodal Officer any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions. (Paragraphs 3 to 5 DOR WMD)

f) Government officers are protected from prosecution or legal proceedings for acts conducted in good faith in pursuance of the WMD Act (section 24 WMD Act). However, there is no explicit prevention of prosecution or legal proceedings of other persons who in good faith take action in relation to assets when implementing the obligations under the WMD Act. India explained that the provision covers government authorities and all the persons acting under the authority of law/order of a government officer- which essentially translates to the extension of protection to every person acting in good faith- under the Act and the Orders under the Act issued by a Government authority based on a plain reading of the statue and related definitions in the WMD Act. There is no case law on point to test this interpretation.

***Criterion 7.3 –***

The DOR WMD places obligations on FIs and DNFBPs to inform the relevant nodal officers, which include regulators of the various REs, where there is a match to a designated individual or entity as well as information surrounding the assets linked to it (Paragraphs 3 to 5 DOR WMD). The nodal officer shall monitor the transactions and accounts of the designated individual or entity so as to prohibit the financing related to the designated individual or entity (Paragraph 5.3 DOR WMD). Section 17 of the WMD Act, makes any violation of Section 12A of the Act a punishable offence with imprisonment for a minimum term of six months to maximum of five years.

The ongoing monitoring of compliance of most FIs and DNFBPs of their obligations under the WMD Act is conducted by their respective regulators and under the specific orders relating to the obligations under s12A WMD Act and the WMD DOR (section 52-53 Master Direction KYC (RBI); SEBI Circular on the Implementation of s12 WMD Act); IRDAI (Circular dated 19th April 2023); PFRDA (Circular dated 2 March 2023); IFSCA (Circular dated 20th October 2023), FIU-IND for VASPs (Guidelines for Professionals dated 4th July 2023 and Guidelines for REs for Providing Services to VDAs) which set out the obligations and sanctions for breaches set out in their respective parent legislation. Sanctions include civil, administrative and criminal penalties depending on the breach'(s47A(1) Banking Regulations Act; Chapter VIA SEBI Act; s3(4), 102 Insurance Act; ss 16,18,28,31 and 32 PFRDA Act; s13 IFSCA Act; ). It remains unclear to what extent DNFBPs are covered.

***Criterion 7.4 –***

a) Listed persons and entities may petition a request for de-listing at the Focal Point Mechanism established under the UNSC Resolution. (Paragraph 7 DOR WMD) The Order as well as details of the procedures under the Order can be found on the FIU website.

b) The DOR WMD lays down the procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism, upon verification that the person or entity involved is not a designated person or entity (Paragraph 7.1 to 7.4 of the DOR WMD Order).

c) The Order lays down the procedure for exemptions to be granted to designated individuals or entities in accordance with UNSCR 1718/2231 or successor resolutions. After satisfaction that the exemption conditions are met and following the due procedures laid out in UNSCRs 1718, 2231 or successor resolutions, the Central Nodal Officer shall communicate to the other Nodal Officers the authorisation granting access to funds or other assets (Paragraph 6 of the DOR WMD Order).

d) The DOR WMD provides the mechanism whereby once the CNO verifies the de-listing, he/she will pass an order to unfreeze the funds/asset within five days and will communicate the order to all Nodal Officers in India. (Paragraphs 7.4 and 9 of DOR WMD).

***Criterion 7.5 –***

a) Accounts of designated individuals or entities to credit interest and other earnings due on those accounts, and that such interest, other earnings and payments continue to be subject to the freezing provisions. (Paragraph 6.2 of P-12011/14/2022-ES Cell-DOR)

b) Payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to freezing obligations under s12A of the WMD Act, in accordance with the sub-criterion (Paragraph 6.2 and 6.3 of 12011/14/2022-ES Cell-DOR).

### *Weighting and Conclusion*

There are no measures in place to protect the rights of *bona fide* third parties acting in good faith, other than government authorities, when implementing obligations under Recommendation 7. The regulators of DNFBPs do not have specific measures for imposing penalties to ensure compliance with the WMD Orders.

**Recommendation 7 is rated largely compliant.**

## Recommendation 8 – Non-profit organisations

In its previous MER, India was non-compliant SR.VIII as no review was undertaken of the adequacy of domestic laws in the NPO sector nor periodic reassessments. There was no outreach to the NPO sector. Only limited information was available on the identity of those who control NPOs and most NPOs were not registered. Measures to sanction violations of rules relating to NPOs were insufficient.

***Criterion 8.1 –***

a) Income of trusts created or institutions established, for charitable or religious purpose, that received more than INR 250 000 (EUR 2778) annually, may be exempt from income tax if they are registered in accordance with section 12AB of the Income Tax Act 1961. The definition of religious purpose is not defined but the definition of charitable purpose is broadly defined and covers the FATF definition. As of March 2023, the ITD has database of 286 260 Indian NPOs established for charitable or religious purpose registered for exemptions which represents the significant spectrum of NPOs within the FATF definition in India.

A sectoral risk assessment of the NPO sector concluded in March 2023 and updated in October 2023, were relied on to identify the subset of NPOs at risk of Information available from the ITD. A combination of data points relating to the geographical location of NPOs, their function (e.g., religious), channels of funding, intelligence information (from IB and other intelligence authorities) relating to their activities that India has used to assess that they pose higher risks of abuse or misuse as well as information obtained based on responses from questionnaires obtained from NPOs.

b) In its National Risk Assessment (which is a restricted document), India has identified six theatres of concern along with the types of potential abuse pertaining to each theatre (which is also referenced in the NPO sectoral risk–assessment) - some of which are cross-cutting and some of which are unique, and which identifies threats linked to the misuse of NPOs.

c) India has taken various measures, including laws and regulations related to NPOs integrity enhancement. The ITD has implemented measures to improve financial transparency. Every NPO filing a tax return, whether or not registered for a tax exemption, is given a PAN which needs to be furnished for transactions over a threshold. NPOs that register under section 12AB of the Income Tax Act are also required to file a statement of donations in respect of donations received. Where an NPO is registered as a society, the NPO must

adhere to the laws under the respective state legislation for societies. These impose accounting audit rules and empower the State Charity Commissioner to obtain information of the charitable entity through the Memorandum of Association, membership and office-holder information etc. Charity Commissioners are able to sanction or dissolve non-functioning NPOs registered as societies, as well as those that have contravened requirements of the Act. Amendments to the Foreign Contribution Regulation Act in 2010 have put in place strong laws and regulations that enhance scrutiny on the foreign contributions received by NPOs although these are not directed solely to mitigate TF risks.

d) However, the measures do not always specifically target the NPO sub-sector that may be abused for TF so that proportionate and effective action is taken to address the risks identified, and no review has been conducted on the adequacy of the measures. While the sectoral risk assessments of the NPO sector review the effectiveness of various measures, including laws and regulations to mitigate the risk of TF abuse of the NPO sector, it is unclear whether the authorities have consequently adapted their adequacy to be able to take proportionate and effective action to address the risks identified.

e) India periodically assesses the vulnerability of the NPO sector to TF in risk assessments in 2019, 2020 and 2022. In March 2023 a sectoral risk assessment of NPOs was conducted, which also in addition, identified the sub-set of NPOs at risk of TF abuse.

***Criterion 8.2 –***

a) NPOs (institutions established for charitable or religious purpose) that register under section 12AB of the Income Tax Act receive a unique Permanent Account Number (PAN) for five years, which needs to be furnished for transactions over a threshold and are required to file a statement of donations in respect of donations received.

Further, if an NPO is a society within the Societies Registration Act (i.e., formed with seven or more persons and established for charitable purposes), it may register under its respective State legislation pertaining to societies. While different States have more specific requirements, this umbrella legislation sets out obligations for maintaining book of accounts, financial statements and other relevant information details regarding the NPO as well as powers for the Charities Commissioner to conduct audits.

NPOs registered under the Foreign Contribution Regulation Act (FCRA) have obligations to provide an audit of the foreign contributions received by the NPO.

b) The ITD has issued a specific guideline that directs its authorities to conduct outreach every 6 months with NPO's. Although this covers the necessity for tax compliance there is also a requirement to address the need to take the necessary steps to prevent abuse of TF, such as limiting activity in accordance with their purpose, understanding the source of donations, implementing internal governance and accountability procedures, financial controls, transparent reporting as well as ensuring that the donations are used towards the purpose of the charity and moving towards financial transactions through banking channels. However, insufficient detail has been provided which shows that such outreach also extends to the donor community.

c) While there is engagement with the NPOs through various country authorities such as ITD and State Charity Commissioners on the implementation of regulations that affect NPOs as well as on risk relating to TF abuse, the authorities do not work with NPOs to develop and refine best practices to address TF risk and vulnerabilities to protect them from TF abuse.

d) Outreach programmes to registered NPOs conducted by ITD have taken place, with the objective of encouraging NPOs to conduct financial transactions through banking channels.

For NPOs registered with ITD, donors can receive tax deductions under s80G of the Income Tax Act. However, in order to promote the use of regulated financial channels, donations made in cash exceeding INR 2000 (EUR 22) are not eligible. Under section 269ST of the Income Tax Act which applies generally, places a INR 200 000 (EUR 2222) daily cash limit on receipt from a person in a single transactional.

***Criterion 8.3 –***

Although India has identified 7 500 NPOs as high risk (see c.8.1(a)), India has not demonstrated that it's supervision or monitoring of NPOs is done in a risk-based manner, targeted at these NPOs at risk of TF abuse.

NPOs that are registered under the ITA, Societies Registration Act and the FCRA have administration and management obligations (See c.8.2(a)), failing which the ITD, Charities Commission and MHA respectively can take remedial action in line with the breach. ITD uses risk-profiling aids (Computer Aided Scrutiny Selection and the Risk Management Strategy) (See ci.10.2) to identify NPOs for enhanced monitoring. While these have uncovered TF related irregularities, the risk-profiling aids are targeted towards uncovering tax irregularities. Thus, it is not clear to what extent the 7500 NPOs as high-risk dovetails with these mechanisms and how they are taken into account in the monitoring and supervision that takes place.

Charity Commissioners are able to sanction or dissolve non-functioning NPOs registered as societies, as well as those that have contravened requirements of the Act but its supervision and monitoring is not focussed on the risk of TF abuse.

As the scope and purpose of the FCRA are broader than, and not primarily intended to prevent TF, the framework under the FCRA it is not risk based in the sense that the regulation and monitoring is in relation to all foreign funding of NPOs, rather than high risk ones or from high-risk origins.

***Criterion 8.4 –***

a) Unlike the Charities Commissions, the ITD has risk-profiling aids which take into account several factors in monitoring including the risk for abuse of TF. The exercise of audit selection is carried out annually. The MHA conducts continuous monitoring of the FCRA based on annual returns, inspection of accounts as well as input received from central security agencies that may include illegal activities such as TF.

b) Under the ITA, non-compliance with obligations is usually addressed through the cancellation of the NPO's registration under section 12AB ITA and/or imposing a range of taxes where tax would have otherwise been exempted. This includes in situations where statements are not maintained or audited. In the last five years, 7,735 cases of violations under ITA were found which resulted in tax liabilities and 87 cases for more serious where NPO registration under Section 12AB have been cancelled. Three irregularities were found

indicating TF linkages and these was shared with the relevant LEA to take criminal action.Under the state legislation relating to the Societies Registration Act, Charities Commission of the respective states have investigative powers into the affairs of societies in their state, as well as access to a broader range of criminal and administrative sanctions against breaches under their legislation, which includes the ability to pursue criminal prosecution against every person (including promoter of company or trust or settlor of the trust) who at the time of the offence was either in charge or responsible for the conduct of the as well as to sanction or dissolve non-functioning NPOs.

The primary measure to address non-compliance with obligations for registered NPOs under the FCRA is the cancellation of the certification, resulting in the NPO not having access to foreign funding. In addition, there are criminal sanctions available to anyone under the FCRA for false declarations. In the last five years, 1828 registrations have been suspended or cancelled and 1260 registrations have not been renewed Nineteen of these have been refused for linkage with organisations supporting terror/radical activities and two registrations have been cancelled due to involvement with terror activities. Most suspensions were due to NPOs' non-compliance with FCRA requirements.

The range of sanctions available under the ITD and Societies Registration Act are effective, proportionate and dissuasive. The sanctions under the FCRA are in line with the broad objectives of FCRA.

Where the NPO is engaged in TF activity, criminal sanctions are available under the Unlawful Activities Prevention Act 1967 (UAPA) (see R.5).

***Criterion 8.5 –***

a) Terrorism and TF intelligence, including intelligence related to NPOs is shared across intelligence agencies in the country through the coordination mechanisms of the MACs, SMACs and FCORD which is available to IB and ITD. This information can be used by MHA and ITD in the monitoring of NPOs registered under the FCRA as well as feeding intelligence information towards ITD's risk-profiling aids. The Charities Commissions share information with SMAC through state authorities.

b) IB is the main agency for intelligence gathering on terrorism and TF, with the National Investigation Agency empowered with broad investigative powers under the NIA Act and the Code of Criminal Procedure to investigate TF and terror related crimes across the states, including NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.

c) For criminal offences including TF related criminal offence, LEAs such as the NIA, have powers under the NIA Act as well as the Code of Criminal Procedure to obtain evidence during the course of an investigation. In addition, there are powers of interview, discovery, inspection, search and seizure for the purposes of the ITA (sections 131- 135 ITA). The FCRA authorises inspection of any account or record maintained on any ground of suspicion of contravention of the FCRA. Charity Commissioners of the respective states are similarly empowered under their respective state legislation to enter on and inspect or cause to be entered on and inspected any property belonging to a public trust, call for and inspect any proceeding of the trustees of a public trust

and all any return, statement, account or report from the trustees or any person connected with public trust.

d) When FIU-IND receives reports from reporting entities on transactions above INR 1 million (EUR 11 111) and where these STRs relate to NPOs or persons related to NPOs, they are processed and disseminated on priority to concerned LEAs based on the risk factors relevant to TF. The MAC coordination mechanism also ensures that LEAs and intelligence authorities are alerted to NPOs involved in terrorism and TF activities.

***Criterion 8.6 –***

India has the ability to exchange information through either MLATs, letters of request issued by an Indian Court or on the basis of assurance of reciprocity. FIU-IND is a member of Egmont and also has 48 MOUs with other countries. Any requests received are examined by the nodal officer in the CTCR division to verify its legal basis, and is then electronically sent to the nodal officers in the Regulators, FIU and nodal officers of the States. (Ministry of Home Affairs Order dated 2nd February 2021.). India's international cooperation framework covers the ability to respond to international requests for information regarding NPOs suspected of TF.

## *Weighting and Conclusion*

India has identified a subset of 7 500 NPOs at risk of TF abuse. Although India supervises its NPO sector for general transparency and good governance purposes, it does not adequately do so based on risk of TF abuse or in a way that targets the subset identified. ITD and State Charity Commissioners do not work with NPOs to develop and refine best practices to address TF risk and vulnerabilities to protect them from TF abuse. Limited evidence exists that the donor community is being educated on potential vulnerabilities of NPOs to TF abuse.

**Recommendation 8 is rated partially compliant**.

## Recommendation 9 – Financial institution secrecy laws

In its last MER, India was rated compliant with the requirements of former R.4.

***Criterion 9.1 –***

Access to information by Competent Authorities

The PMLA requires all reporting entities (REs) to maintain and provide information on transactions, accounts, identity of its clients and beneficial owners and business correspondence relating to their clients to the Director of the FIU (PMLA, s.12(1); Notification G.S.R. 440(E) of 1 July 2005). In addition, the Director of FIU has powers to request REs to provide additional records and information as necessary for the purposes of PMLA (s.12A). The PMLA further establishes that its provisions shall have effect notwithstanding inconsistent provisions of any other law (PMLA, s.71).

Financial sector regulators have powers to request documents and information relating to respective FIs that they supervise. These powers are set out in detail in R.27.

Exchange of information between competent authorities

The Director of the FIU is authorised to share relevant information with authorities, officers or bodies performing any function, relating to (i) imposition of any tax, duty or levy; (ii) dealings in foreign exchange; (iii) prevention of illicit traffic in the narcotic drugs and psychotropic substances under the Narcotic Drugs and Psychotropic Substances Act, 1985 (PMLA, s.66(1)). In addition, the Director may also share information with other officer, authority or body for

performing functions under other law, as notified by the Central Government (PMLA, s.66(1)). Over 25 authorities have been notified under the referenced provision.[146] The FIU Director and the above-mentioned authorities are authorised to share information with other concerned agencies for necessary action, if they are of the opinion that provisions of any other law are contravened and illegal activity may be taking place, such as money laundering terrorist financing and associated predicate offences (PMLA, s.66(2)).

In addition, the Central Government may enter into an agreement with the Government of any country outside of India for exchange of information for the prevention or investigation of offences under the PMLA or under the corresponding law in force in the other country (PMLA, s.56). Financial sector regulators have entered into arrangements such as MoUs and exchange of letters on supervisory co-operation to share information with foreign counterparts, as set out in R.40 in greater detail.

Sharing of information between FIs

There are no restrictions on the sharing of information between financial institutions where this is required by R.13, R.16 and R.17.

### *Weighting and Conclusion*

All criteria are met.

**India is rated Compliant with Recommendation 9.**

## Recommendation 10 – Customer due diligence

In its last MER, India was rated partially compliant with the requirements of former R.5. Whilst several deficiencies were identified in that report, India's 8th FUR of June 2013 concluded that these deficiencies had been addressed and that India's level of compliance with R.5 was essentially equivalent to LC.

Some requirements related to R.10 are set up in the PMLA and supplemented by the PML Rules. Many PMLA provisions specify that further aspects will be prescribed by the central government. The framework is further supplemented by sectoral regulations (see below), issued under the PML Rules. PML Rule 9(14) specifies that regulators shall issue guidelines incorporating the requirements of related to the verification of customer records and may prescribe enhanced or simplified measures.[147]

| Sector | Regulator | Reference |
|---|---|---|
| Banking, MVTS | RBI | RBI's Master Direction on KYC |

[146] Including the ED, Cabinet Secretariat (Research and Analysis Wing), MHA, National Security Council Secretariat, IB, Economic Offences Wing of CBI, Chief Secretaries of the State Governments, NIA, SFIO, Military Intelligence, Defence Intelligence Agency, State Police Department, Director General of Foreign Trade, MEA, Special Investigation Team, GST Network, National Technical Research Organisation, The National Intelligence Grid, Central Vigilance Commission, Competition Commission of India, Department of Company Affairs, RBI SEBI, IRDAI, other AML/CFT Regulators.

[147] In the case of GJ Fernandez vs. State of Mysore & Ors 1967 AIR 1753, the Indian Supreme Court held that in order for executive directions, guidelines to have the force of statutory rules it must be shown that they have been issued either under the authority conferred by some statute, or under some provision of the Constitution.

| | | |
|---|---|---|
| Securities | SEBI | SEBI's Master Circular on AML/CFT |
| Insurance | IRDAI | IRDAI's Master Guidelines on AML/CFT |
| Pension | PFRDA | PFRDA's Guidelines on AML/CFT |
| International Financial Services Centre | IFSCA | IFSCA's Guidelines on AML/CFT |

***Criterion 10.1*** – FIs are prohibited from opening or keeping anonymous accounts or accounts in fictitious names (PML Rules, Rule 9(11)).

***Criterion 10.2*** – FIs are required to undertake CDD measures when:

a) commencing an account-based relationship (PML Rule 9(1));

b) carrying out transactions of an amount equal to or exceeding INR 50 000 (EUR 563), whether conducted as a single transaction or several transactions that appear to be connected (PML Rule 9(1)).

c) carrying out international money transfers (PML Rule 9(1)). In addition, the FI regulators directions/ guidelines contain CDD obligations in respect of wire transfers in general;

d) there is suspicion of ML or TF (PML Rule 9(12)(ii));

e) there are doubts about the adequacy or veracity of previously obtained client identification data (Rule 9(12)(ii)).

***Criterion 10.3*** – FIs are required to identify their customers and verify their identity using officially validated identity documentation, as prescribed in the PML Rules (PMLA, ss.12(e) and 11A). Under these, FIs are required to identify their customers (PML Rules 3, 4 and 9) and to verify the customers' identity using reliable and independent sources of identification when (i) commencing an account-based relationship, (ii) carrying out transactions equal or over INR 50 000 (EUR 563) or (iii) international money transfer operations (PML Rule 9(1)(a)). In addition, for banks and other FIs regulated by the RBI, no transaction can be undertaken without following the CDD procedure, which involves identifying and verifying the customer (RBI's Master Direction on KYC, paras. 10 and 3(b)(v)).

PML Rule 9 prescribes various sources and documents which are acceptable for verification of identity, which represents reliable, independent sources of identification data. Prescribed documentation includes an Aadhaar number or other officially valid document for individuals[148], a certificate of incorporation for companies and a registration certificate for partnerships and trusts (PML Rule 9 (4), (6-10)).

FIs are required to file, within 10 days of the commencement of an account relationship, a customer's identity record with the Central KYC Records Registry ("Central KYC Registry"). That Registry issues a unique KYC Identifier for each customer (Rule 9(1B)). Where a customer already holds a KYC Identifier, the client does not need to resubmit identification documents to the FI and can simply inform their KYC Identifier, subject to exceptions (Rule 9(1C)). FIs are nonetheless required to obtain additional or updated information, where (i) there is a change in the customer information recorded in the Central KYC Registry; or (ii) FIs considers it necessary in order to verify the identity or address of the client, or to perform EDD, or to build an

[148] Aadhaar is a 12-digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India. The number serves as a proof of identity and address, anywhere in India.

appropriate risk profile of the client ((Rule 9(1C)). After obtaining additional or updated information from a customer in the cases referenced above, FIs are required to, as soon as possible, furnish such information to the KYC Registry (Rule 9(1D)). The Central KYC Registry is required to send an electronic notification of the update of customer information to all REs which have dealt with the concerned client (Rule 9(1D)).

There are some exceptions to the requirement to verify the customer identity using reliable and independent identification data:

- *Small accounts:* Individuals may open a "small account"[149] by producing a self-attested photograph and affix a signature or thumb print, provided that some conditions are met, including that a bank designated officer, while opening the small account, certifies under his or her signature that the person opening the account has affixed his signature or thumb print in his or her presence (PML Rule 9(5)). Banks are required to monitor "small accounts" and, where there is ML/TF suspicion or other high-risk scenarios, they are required to establish the identity of the customer as done in relation to other accounts (RBI's Master Direction for KYC, ss.23(h)). Small accounts were considered as low risk in the 2022 NRA (see c.10.18).
- *Prepaid Payment Instruments (PPIs):* Small PPIs, including digital wallets, of maximum monthly amount of INR 10 000 (EUR 120) are subject to simplified CDD, which involves the collection of a mobile number, one-time password and self-declaration of name and ID number (RBI's Master Direction on PPIs, para.9.1). PPIs were considered medium-low risk in the 2022 NRA.

***Criterion 10.4 –*** When the client purports to act on behalf of a legal person, natural person or trust, the FI is required to (i) verify that any person purporting to act on behalf of such client is so authorised and (ii) identify and verify the identity of that person (PML Rule 9(10)). It is not clear if how this requirement applies where the client is a legal arrangement other than a trust, since it is not referenced in that provision. However, the PML Rules also provide that, where the client is an unincorporated association or a body of individuals, the RE is required verify such documents for the person holding an attorney to transact on its behalf (PML Rules 9(9)(iv)).

***Criterion 10.5 –*** FIs are required to verify the identity of beneficial owners by verifying officially valid identity documentation (PMLA, s.11A). Further, at the time of commencement of an account-based relationship, carrying out transactions equal or over INR 50 000 (EUR 563) or international money transfer operations, FIs are required to o determine whether a client is acting on behalf of a beneficial owner, identify the beneficial owner and take all steps to verify his or her identity, using reliable and independent sources of identification (Rule 9(1)(a)).

Beneficial owner is defined in the PMLA as an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and *includes* a person who exercises ultimate effective control over a 'juridical' person (PMLA, s.2(1)(fa)). It is not clear if the definition includes a natural person who exercises ultimate effective control over a legal arrangement; however, the PML Rules clarify how the beneficial owner of trusts and other legal arrangements should be identified (see c.10.11 below).

[149] A "small account" is a savings account in a banking company where (i) the aggregate of all credits in a financial year does not exceed INR 100 000 (EUR 1123); (i) the aggregate of all withdrawals and transfers in a month does not exceed INR 10 000 (EUR 112); and the balance at any point of time does not exceed INR 50 000 (EUR 562). This limit on balance is not considered while making deposits through government grants, welfare benefits and payment against procurements (Rule 2(1)(fc)).

***Criterion 10.6 –*** FIs are required to understand the purpose and intended nature of the business relationship (PML Rules, Rule 9(1)(a)(i)).

***Criterion 10.7 –***

a) FIs are required to exercise ongoing due diligence with respect to business relationships with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, their business and risk profile and, where necessary, the source of funds (PML Rule 9(12)(i)).

b) FIs are required to apply due diligence measures to existing clients on the basis of materiality and risk and conduct due diligence on such existing relationships at appropriate times or as may be specified by the regulator, taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained, such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly where there is high risk (PML Rule 9(12)(iii)).

The framework is supplemented by sector specific regulations.

*Banking sector*: Banks and other FIs regulated by the RBI are required to adopt a risk-based approach for "periodic updation" of KYC. ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk (RBI's Master Direction on KYC, para. 38). "Periodic updation" is defined as steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI (para. 3(b) xiii.). RBI prescribes that updates should be carried at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC update (para. 38) (See Immediate Outcome 4).

*Securities:* Securities intermediaries are required to periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk clients (SEBI's Master Circular on AML/CFT, para 11 (viii)).

*Insurance*: Insurance companies and intermediaries are required to conduct CDD for existing customers from time-to-time based on the adequacy of the data previously obtained such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk clients (IRDAI's Master Guidelines on AML/CFT, para. Para 8.2.2).

*Pension sector*: FIs in the pension sector are required to conduct CDD for the existing customers from time-to-time based on the adequacy of the data previously obtained such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk clients. In addition, periodic updates of NPS accounts are required to do every three, two years or only at the time of exit, depending on the type of account (PFRDA's Guidelines on AML/CFT, para. 8.2.1 and 8.2.2.1).

*IFSC*: FIs in the IFSC are required to ensure that the CDD data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing CDD data, documents and information, particularly for customers with high-risk rating (IFSCA's Guidelines on AML/CFT, para. 5.8 (vii)).

***Criterion 10.8 –*** FIs are required to take reasonable steps to understand the nature of the customer's business, and its ownership and control (PML Rule 9(1)(b)).

***Criterion 10.9 –*** PML Rules 9(6)-(9) detail the information and documents FIs need to collect to identify a customer and verify its identity. The requirements are tailored to each category of customer (i.e., company, partnership firm, trust, unincorporated association or body of individuals). They require documentation that attest name, legal form and proof of existence, address of the registered office, and if different, a principal place of business be collected. For a company, this also includes a resolution from the board of directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on the company's behalf, and the names of the persons holding a senior management position.[150]

***Criterion 10.10 –***

PML Rule 9(3) prescribes the information to determine the beneficial owner for different types of legal persons. Where the client is a **company,** the beneficial owner is determined as follows (Rule 9(3)(a)):

- the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more 'juridical' person, has a controlling ownership interest or who exercises control through other means. Where no natural person is identified the provision above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
- "Controlling ownership interest" means ownership of or entitlement to more than 10% of shares or capital or profits of the company;
- "Control" includes the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

Where the client is **a partnership firm**, the beneficial owner is considered to be the natural person(s), who, whether acting alone or together, or through one or more 'juridical' person, has ownership of/entitlement to more than 15% percent of capital or profits of the partnership or who exercises control through other means (PML Rule 9(3)(b)).

Where the client or the owner of the controlling interest is an **entity listed on a stock exchange** in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities (PML Rule 9(3)(f)). Indian companies listed on a stock exchange are subject to the beneficial ownership requirements provided in the Companies Act[151], as analysed in c.24.6.

---

[150] The following documentation is also required to be collected in relation to other type of customers:
For partnership firms, the partnership deed, names of all the partners and identity information of managers, officers or employees, as the case may be, of the person holding an attorney to transact on the partnership's behalf;
For trusts, trust deed, list of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust.
For unincorporated association or a body of individuals, resolution of the managing body of such association or body of individuals, identity information of managers, officers or employees, as the case may be, of the person holding an attorney to transact on the association's/body's behalf.

[151] SEBI Circulars SEBI/HO/CFD/CMD1/CIR/P/2018/149 and SEBI/HO/CFD/CMD1/CIR/P/2019/36.

***Criterion 10.11 –*** Where the client is a **trust**, FIs are required to identify the beneficial owner(s) through the following information: identification of the trustee, settlor, the beneficiaries with 10% percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership (PML Rule 9(3)(e)). In addition, FIs are also required to collect information on the names of the beneficiaries, trustees, settlor, protector (if any) and authors of the trust (PML Rule 9(8)(v)).

Where the client is an **unincorporated association** or **body of individuals,** the beneficial owner is considered to be the natural person who has ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals ((PML Rule 9(3)(c)). Where no natural person is identified under the rule above, the beneficial owner is the relevant natural person who holds the position of senior managing official (PML Rule 9(3)(c)).

***Criterion 10.12 –*** Insurers and insurance intermediaries are required to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies:

a) as soon as a beneficiary of a life policy is identified as a specifically named natural person, legal person or legal arrangement, obtain the full name of such beneficiary (IRDAI AML/CFT Guidelines, para 8.2.4.2(i); IFSCA Guidelines on AML/CFT, para 5.4.9(i)).

b) in relation to beneficiary(ies) that is designated by characteristics or by class or by other means, obtain sufficient information concerning the beneficiary to satisfy themselves that they will be able to establish the identity of the beneficiary at the time of the payout (IRDAI AML/CFT Guidelines, para 8.2.4.2(ii); IFSCA Guidelines on AML/CFT, para 5.4.9(ii)).

c) for both the above cases, verify the identity of the beneficiary at the time of the payout (IRDAI AML/CFT Guidelines, para 8.2.4.2(iii); IFSCA Guidelines on AML/CFT, para 5.4.9, Guidance Note (1)).

***Criterion 10.13 –*** Insurers in India are required to carry out necessary CDD, if required, of the policyholders/beneficiaries/legal heirs/assignees including beneficial owner, if any, before making the pay-outs. Insurers are required to take reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary including performing EDD, *if required*, in case the insurers determine that a beneficiary presents a higher risk, at the time of payout. (IRDAI's Master Guidelines on AML/CFT, para. 8.2.4.2). The term "if required" appears to weaken the provision.

*IFSC* insurance undertakings are required to include the beneficiary of a life insurance policy as a relevant risk factor included in determining whether enhanced CDD measures are applicable (IFSCA's AML/CFT Guidelines, Guidance Note 3 to para. 5.4.9). If the IFSC insurance undertaking determines that a beneficiary who is a legal person or a legal arrangement presents a high risk, then the enhanced CDD measures must be carried out, including reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out.

***Criterion 10.14 –***

FIs are required to verify the customer and beneficial owners' identity (PMLA, s.11A). As detailed in the PML Rules, FIs are required to verify the identity of the customer and beneficial owner at the time of commencement of an account-based relationship, when carrying out transactions of equal or over INR 50 000 (EUR 563) or international money transfers (PML Rule 9(1)). FI regulators may permit FIs to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the regulator is of the view that ML/TF

risks are effectively managed and where this is essential not to interrupt the normal conduct of business (Rule 9(1)).

In relation to the IFSC, the IFSCA Guidelines state that CDD should be conducted, as soon as reasonably practicable and, in no event, it should exceed 30 business days after the establishment of business relationship (IFSC Guidelines on AML/CFT, para 5.3).

Small PPIs, including digital wallets, of maximum monthly amount of INR 10 000 (EUR 120) are subject to a deferred (full) CDD up to a period of 24 months (see c.10.3). At the time of opening such wallets, simplified CDD applies, involving the collection of the following information: a mobile number, one-time password and self-declaration of name and ID number (RBI's Master Direction on PPIs, para.9.1). Whilst this does not amount to performing CDD as soon as reasonably practicable as is required, risk mitigation measures are in place. PPIs are only allowed for purchase of goods and services at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer to accept the PPIs as payment instruments. Further, funds transfer or cash withdrawal from such PPIs is not permitted.

In relation to small accounts[152] Non-Banking Finance Companies (NBFCs) are required may open accounts with the information and under similar conditions explained in c.10.3 in relation of small accounts in banks. NBFCs are nonetheless required to perform regular CDD within one year from opening the account (RBI's Master Direction for KYC, s.24).

***Criterion 10.15 –*** There is no general requirement in place for FIs to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification, except for the IFSC. However, this does not represent a shortcoming as other FI Regulators in India require FIs to complete customer verification before a customer can utilise the business relationship (RBI's Master Direction on KYC, Para. 10; SEBI's Master Circular on AML/CFT, Para 11(A); IRDAI's Master Guidelines on AML/CFT, Para 8.2.1; PFRDA's Guidelines on AML/CFT, Para 8.2.1). In the cases described under c.10.14 and c.10.3 (e.g., small accounts and small PPIs), there are some mitigating measures in place. IFSC FIs are required to ensure that their AML/CFT systems and controls include internal risk management policies and procedures concerning the conditions under which such business relationships may be established with a customer before completing verification (IFSCA Guidelines on AML/CFT, para 5.3(e)).

**Criterion 10.16 –** FIs are required to apply CDD measures on existing clients on the basis of materiality and risk and conduct due diligence on such relationship at appropriate times taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained (Rule 9(12)(iii) of PML Rules).

**Criterion 10.17 –** FIs are required to perform EDD in respect of specified transactions (PMLA, s.12AA). Specified transactions include transactions or class of transactions where there is a high-risk or where there is ML or TF, as may be prescribed. EDD includes additional steps to examine the ownership and financial position, including sources of funds of the client, and to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties (PMLA, s.12AA). The PML Rules enables the regulator to issue guidelines to prescribe enhanced measures based on overall ML/TF risks

[152] The aggregate balance in all accounts held in an individual in a NBFC shall not exceed INR 50 000 (EUR 562) and the aggregate credit shall not exceed INR 100 000 (EUR 1123) in a year.

(Rule 9(14)(i)). Regulators have issued such guidelines, some of them detailing higher-risk scenarios.[153]

***Criterion 10.18*** – The PML Rules enables FI Regulators to issue guidelines to prescribe simplified measures to verify the client's identity taking into consideration the type of client, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved (Rule 9(14)(i) of the PML Rules). Moreover, simplified measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply or where the risk identified is not consistent with the NRA (PML Rules' Explanation to Rule 9(14)(i)). All regulators have issued guidelines on simplified DD measures, mostly intended to promote financial inclusion or based on materiality of transactions or where ML/TF risks are identified to be low.[154] For banks and FIs regulated by the RBI, simplified DD measures are provided in respect of "small accounts", accounts maintained with NBFCs, small PPIs[155] and accounts for self-help groups and foreign students. For small PPIs, a medium-low risk has been identified in the NRA, however.

***Criterion 10.19 –***

a) All FIs are required not to open an account on behalf of other persons whose identity has not been disclosed or cannot be verified (PML Rules 9(11)). In addition, FIs are required not to perform a transaction (i.e., for customers that have already been onboarded or are undertaking an occasional transaction); or to terminate the business relationship when they are unable to comply with relevant CDD measures (RBI Master Direction on KYC, paras. 10(b-c); SEBI Master Circular on AML/CFT, para. 11A and 12(v); IRDAI's Master Guidelines on AML/CFT, para. 8.2.1 and 8.1.12; PFRDA's Guidelines on AML/CFT, para.8.1.4; IFSCA's Guidelines on AML/CFT, Paras. 5.3 and 5.10).

b) All FIs are required to consider filing an STR when they are unable to comply with relevant CDD measures (RBI Master Direction on KYC, para. 10(b); SEBI Master Circular on AML/CFT, para. 12(v); IRDAI's Master Guidelines on AML/CFT, para. 8.2.1 and 8.1.12; PFRDA's Guidelines on AML/CFT, para.8.1.4; IFSCA's Guidelines on AML/CFT, paras. 5.3 and 5.10).

***Criterion 10.20 –***

All FIs are permitted not to pursue the CDD process, where they have a suspicion of ML/TF, and they reasonably believe that performing the CDD process will tip-off the customer and are required to file an STR (RBI Master Direction on KYC, para 11A; SEBI's Master Circular on AML/CFT, para. 11(x); IRDAI's Master Guidelines on AML/CFT, para 8.2.6; PFRDA's Master Guidelines on AML/CFT, para. 8.2.2.3; IFSCA Guidelines on AML/CFT, para 5.10).

## *Weighting and Conclusion*

While most of India's CDD measures meet the FATF Standards, minor shortcomings exist. Those include exceptions to the requirement to verify the customer identity using reliable and

[153] RBI's Master Direction on KYC, Paras 36, 37, 40 to 42 and 63(i); SEBI's Master Circular on AML/CFT, Paras 12(ii), 20 and 21; IRDAI's Master Guidelines on AML/CFT, Para 11; PFRDA's Guidelines on AML/CFT, Para 8.2.2.2; IFSCA's Guidelines on AML/CFT, Para 5.6.

[154] RBI's Master Direction on KYC, Paras 23, 24, 43 and 44; SEBI's Master Circular on AML/CFT, Para. 21; IRDAI's Master Guidelines on AML/CFT, Para 10.1; PFRDA's Guidelines on AML/CFT, Para 10.1; IFSCA's Guidelines on AML/CFT, Para 5.7.

[155] This refers to small PPIs without a cash loading facility. Those PPIs can be loaded/ reloaded from a bank account or credit card.

independent identification data, or CDD deferral in connection with certain financial inclusion products such as small accounts as well as small PPIs. In addition, there are small gaps on the CDD rules applicable to CDD for beneficiaries of life insurance policies.

**India is rated Largely Compliant with Recommendation 10.**

### Recommendation 11 – Record-keeping

In its last MER, India was rated as largely compliant with the previous R.10 because of the PMLA did 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 was not contained in law or regulation; and sector specific circulars had exempted some insurance products, including term life policies, from AML requirements. The 8th FUR of India noted that the scope deficiency in respect of commodities future brokers had been addressed as a result of the PMLA amendments that came into force in February 2013.

***Criterion 11.1 –***

FIs are required to maintain records of all transactions, both domestic and international, for a period of five years from the date of transaction between a client and the FI (PMLA, s.12(1), PML Rule 3).

***Criterion 11.2 –***

FIs are required to maintain records of documents evidencing identity of clients and beneficial owners, as well as account files and business correspondence relating to clients (PMLA, s.12(1)), as well as results of any analysis undertaken (PML Rule 10(3)). Records must be kept for a period of five years after the business relationship between a client and the FI has ended or the account has been closed, whichever is later (PMLA, s.12(4) and s.12(1)(e)). There is no distinction between account based and occasional transactions for record management requirements.

***Criterion 11.3 –***

FIs are required to maintain records of all transactions, in such manner as to enable it to reconstruct individual transactions for a period of five years from the date of transaction (PMLA, s.12(1); PML Rule 3).

***Criterion 11.4 –***

Under section 12A of the PMLA, the Director of the FIU is empowered to request the records pertaining to identity of clients and transaction and any additional information within such time and in such manner as the Director may specify from any FI. There are sanctions for failure of the FIs to provide the information (PMLA, s.13(2), as noted under c.35.1).

The powers of LEAs to seek information and transaction records from FIs is detailed in response to R.31.

### *Weighting and Conclusion*

**India is rated Compliant with Recommendation 11**

### Recommendation 12 – Politically exposed persons

In its last MER, India was rated as partially compliant with the previous R.6. Its 8th FUR concluded that India had addressed nearly all of the technical deficiencies and its level of compliance was therefore with essentially equivalent to LC. The remaining deficiency referred to the absence of a requirement in the RBI circulars to apply enhanced measures to close associates of PEPs.

***Criterion 12.1*** – PEPs are defined as individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials (Rule 2(db), PML Rules). All FIs are required to:

a) put in place risk management systems to determine whether a customer or the beneficial owner is a PEP.156

b) obtain senior management approval before establishing (or continuing, for existing customers) business relationships with foreign PEPs.157

c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs. For banks and other RBI FIs, the requirement refers to "source of funds/ wealth", leading to questions on whether FIs are required to establish both;158 and

d) All FIs are required to conduct enhanced ongoing monitoring on the relationship with a foreign PEP[159].

***Criterion 12.2*** – The PMLA, PML Rules as well as the directions/guidelines issued by most FI sector Regulators (RBI, SEBI, IRDAI and PFRDA) have no specific provisions dealing with domestic PEPs or persons who or have been entrusted with a prominent function by an international organisation. In relation to *IFSC* FIs, the IFSCA Guidelines on AML/CFT do not provide for a distinction between foreign and domestic PEPs[160] and the measures that apply to foreign PEPs described under c.12.1 above also apply to domestic PEPs (para. 5.5).

Regulators require FIs to categorise customers based on the FI's assessment and risk perception. In their risk categorisation, FIs are required to consider parameters such as customer's identity, social/financial status, nature of business activity. India considers that on that basis FIs would already consider domestic PEPs in their risk management policies; however, this does not amount to a specific requirement.

***Criterion 12.3*** – *IFSC* FIs are required to apply the relevant requirements of criteria 12.1 and 12.2 to family members or close associates of all types of PEPs (IFSCA Guidelines on AML/CFT, para. 5.5).

156 RBI's Master Direction on KYC, para. 41A(a); SEBI's Master Circular on AML/CFT, para. 14; IRDAI's Master Guidelines on AML/CFT, para. 14; PFRDA's Guidelines on AML/CFT, para. 14; IFSCA's Guidelines on AML/CFT, para. 5.5.

157 RBI's Master Direction on KYC, para. 41; SEBI's Master Circular on AML/CFT, para. 14; IRDAI's Master Guidelines on AML/CFT, para. 14; PFRDA's Guidelines on AML/CFT, para.14; IFSCA's Guidelines on AML/CFT, para. 5.5.

158 RBI's Master Direction on KYC, para. 35, 41A & B; SEBI's Master Circular on AML/CFT, para. 14; IRDAI's Master Guidelines on AML/CFT, para. 14.4; PFRDA's Guidelines on AML/CFT, para. 14.4; IFSCA's Guidelines on AML/CFT, para. 5.5.

159 Para 41 of RBI's Master Direction on KYC, Paras 11(vi) and 12(iii)(e) of SEBI' Master Circular on AML/CFT, Para 14 of IRDAI's Master Guidelines on AML/CFT, Para 14 of PFRDA's Guidelines on AML/CFT, Para. 5.5 of IFSCA's Guidelines on AML/CFT.

160 Pursuant to para. 1.3.34. "Politically Exposed Person" means the individuals who are or have been entrusted with prominent public functions by any country, which shall include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or International Organisation Politically Exposed Person.

Other FIs in India are required to apply the relevant requirements of criteria 12.1 to family members or close relatives/associates of foreign PEPs.[161] The deficiencies identified in respect of c.12.2 would also have a bearing here, as FIs other than *IFSC* FIs are not required to apply relevant requirements to domestic PEPs or their family members and close associates.

***Criterion 12.4 –*** Only FIs regulated by IRDAI and IFSCA can issue life insurance policies. Insurers regulated by the IRDAI are required to lay down appropriate on-going risk management procedures for identifying and EDD measures on an on-going basis to PEPs and customers who are family members, close relatives/associates of PEPs (IRDAI's Master Guidelines on AML/CFT, para 14.2). These measures are also applicable to insurance contracts of which a PEP is the beneficial owner(s) (para. 14.2). If the on-going risk management procedures indicate that the customer or beneficial owner(s) is found to be a PEP, or subsequently becomes a PEP, the senior management should be informed of this business relationship and apply EDD measures should apply (para.14.3). Insurers are also required to carry out necessary due diligence of beneficiaries before making the pay-outs of life insurance policies (para. 8.2.4, IRDAI's Master Guidelines on AML/CFT). In addition, where higher risks are identified, insurers should consider filing an STR (para.8.2.5). However, as noted in c.12.2 above, a PEP would refer only to a foreign PEP (and as such no requirements would apply in relation to domestic PEPs).

Insurers in the IFSC "should be required" to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a STR (IFSCA's Guidelines on AML/CFT, para.5.4.9(iii)).

### *Weighting and Conclusion*

The lack of coverage of domestic PEPs is a significant shortcoming, considering India's risk and context, and also impacts compliance with c.12.3 and c.12.4.

**Recommendation 12 is rated Partially Compliant.**

## Recommendation 13 – Correspondent banking

In its last MER, India was rated as partially compliant with the previous R.7, because it did not provide evidence that implementation was effective.

***Criterion 13.1 –*** In relation to cross-border correspondent banking and other similar relationships, FIs are required to:

a) gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action (RBI's Master Direction on KYC, para. 63(a); (IFSCA's Guidelines on AML/CFT, para 7.1).

b) assess the respondent bank's AML/CFT controls (RBI's Master Direction on KYC, para. 63(a); IFSCA's Guidelines on AML/CFT, para 7.1(iii)).

[161] Para. 41A of RBI's Master Direction on KYC, Para. 12(iii)(e) of SEBI' Master Circular on AML/CFT, Para. 14.2 of IRDAI's Master Guidelines on AML/CFT, Para. 14.2 of PFRDA's Guidelines on AML/CFT.

c) obtain approval from senior management before establishing new correspondent relationships (RBI's Master Direction on KYC, para. 63(b); IFSCA's Guidelines on AML/CFT, para 7.1).

d) understand and document the respective AML/CFT responsibilities of each institution (RBI's Master Direction on KYC, para. 63(c); IFSCA's Guidelines on AML/CFT, para 7.1).

***Criterion 13.2*** – With respect to "payable-through accounts", FIs regulated by both RBI and IFSCA are required to satisfy themselves that the respondent bank: (a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank and is undertaking on-going 'due diligence' on them; and (b) is able to provide relevant CDD information immediately upon request to the correspondent bank (RBI's Master Direction on KYC, para. 63(d)(e); IFSCA's Guidelines on AML/CFT, para 7.1(d)(e)).

***Criterion 13.3*** – FIs regulated by both RBI and IFSCA are prohibited from entering into correspondent banking relationships with shell banks (RBI's Master Direction on KYC, para. 63(f); IFSCA's Guidelines on AML/CFT, para 7.1(f)). There is no express prohibition for FIs to continue correspondent banking relationships with shell banks, but FIs regulated are required to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks (RBI's Master Direction on KYC, para. 63(h); IFSCA's Guidelines on AML/CFT, para 7.1(g)).

The definitions of "shell bank" and "physical presence" in the RBI's Master Direction on KYC and IFSCA's Guidelines on AML/CFT mirror the definitions of the FATF Glossary.

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 13 is rated Compliant.**

## Recommendation 14 – Money or value transfer services

In its last MER, India was rated largely compliant with the requirements of former SR.V1, because the application of the FATF Recommendations to MVTS providers suffered from the same deficiencies as identified in relation to the rest of the financial sector.

***Criterion 14.1*** – Different types of MVTS are available in India and they require license (authorisation) or registration with the RBI:

- *Payment System Operators*[162] (PSOs), requires authorisation under Payment and Settlement Systems Act, 2007 (PSS Act, s.4);
- Authorised dealers in foreign exchange, money changers or offshore banking unit (Foreign Exchange Management Act, 1999 (FEMA), s.10(1)).
- *Money Transfer Service Scheme (MTSS)* (FEMA and RBI's Master Direction on MTSS).

[162] This includes: financial market infrastructures, retail payments organisations, card payment networks, cross-border inbound money transfer entities, Automated Teller Machine (ATM) networks, white label ATM operators, Prepaid Payment Instrument (PPI) issuers, instant money transfer service provider, Trade Receivables Discounting System operators, Bharat Bill Payment Central Unit, Bharat Bill Payment Operating Units.

MTSS is a mechanism for transferring personal remittances from overseas to beneficiaries in India only (RBI's Master Direction on MTSS). This scheme involves Overseas Principals, which are required to obtain an authorisation from the RBI (para.4) to operate a payment system.

Indian agents are required to be registered or licensed with the RBI (para. 3) as a bank or other authorised dealer in foreign exchange, full fledged money changer or be the Department of Posts. Indian agents can appoint sub-agents and are required inform such appointments to the RBI (para. 5). The RBI maintains a list of appointed agents and sub-agents in its website.

***Criterion 14.2 –*** *PSOs*: Any person found operating a payment system without authorisation from the RBI is liable to imprisonment for a term which shall not be less than one month, but which may extend to ten years; a fine which may extend to INR 10 million (EUR 111 560) or both. An additional fine which may extend to INR 100 000 (EUR 1 115) for every day, after the first, during which the contravention or failure to comply continues may be added (PSS Act, s. 26).

*Authorised dealers in foreign exchange*: Any person that carries on business of cross-border money transfer to India without authorisation is, upon adjudication, liable to a penalty (i) up to three times the sum involved in such contravention where such amount is quantifiable, or (ii) up to INR 200 000 (EUR 2 231) where the amount is not quantifiable. Where the contravention is a continuing one, an additional penalty up to INR 5 000 (EUR 56) may be imposed for every day after the first day during which the contravention continues (FEMA, s.13(1)). Whilst the penalties applicable to instances where the contravention amount is not quantifiable may not be dissuasive for larger businesses, the operating without a license and carrying transactions in this context would normally have a quantifiable impact.

To identify unauthorised FIs, the RBI relies on market intelligence (normally shared by authorised entities) or complaints, and work of LEAs to disrupt hawala and other informal networks. The RBI also publishes a list of authorised entities in its website and there is a portal where any citizen can file a complaint about an unauthorised FI. The ED, for instance, has dedicated units that collect intelligence, including on hawala, and can also receive anonymous complaints. The ED and other LEAs have a strong focus on the investigation of hawala networks where remittances are used to launder money or to finance terrorism activities or where organised criminal organisations are involved. This is evidenced by a varied of case studies of successful investigation and prosecution of hawaladars operating in India included in the analysis of Immediate Outcomes 7 and 9.

***Criterion 14.3 –*** *PSOs and Authorised dealers in foreign exchange:* PSOs and persons authorised to deal in foreign exchange are subject to monitoring by the RBI for compliance with AML/CFT obligations.

*MTSS:* Indian Agents and their Sub-agents are subject to '*mutatis mutandis*' the RBI's Master Direction on KYC (Para 8, Master Direction on MTSS).

***Criterion 14.4 –*** *PSOs including PPIs:* PSOs are required to maintain a central record of all outsourcing arrangements. PPIs issuers are permitted to load / reload PPIs through their authorised/ designated agents, subject to conditions, including that issuers carry proper due diligence on the persons appointed as agents (RBI's Master Directions on PPIs, para.7.9). PPI issuers are also required to display the detailed list of its authorised / designated agents on the website or mobile app (para.16.2).

*Authorised dealers in foreign exchange:* They are required to maintain a current list of its agents/ franchisees and report it to RBI. RBI's approval is required for the first franchisee agreement (RBI Master Direction on Money Changing Activities, section 3).

*MTSS:* Indian Agents of MTSS are required to be authorised or licensed by the RBI (para. 3). Only authorised dealers in foreign exchange (categories 1 and 2), full-fledged money changers, scheduled commercial banks and the Department of Posts can be MTSS Agents. Agents can appoint sub-agents and are required inform the RBI of appointments made during a quarter within 15 days from the end of the quarter (Master Direction on MTSS, para. 5).

***Criterion 14.5 –*** *PPI issuers:* They are permitted to load/ reload PPIs through their authorised/ designated agents, subject to conditions, including adherence to AML/CFT norms; and remaining responsible as the principal for all acts of omission or commission of their agents (RBI's Master Directions on PPIs, para.7.9). There are, however, no specific requirements for PPI issuers to include their agents in the issuers' AML/CFT programmes and monitor them for compliance with these programmes.

*Other PSOs:* As per the Terms and Conditions of the Certificate of Authorisation, PSOs are responsible and accountable for the transactions/actions undertaken by their authorised agents, retail outlets and merchants. However, this does not amount to a requirement for PSOs to include their agents in their AML/CFT programmes and monitor the agents for compliance with these programmes.

*Authorised dealers in foreign exchange:* Agents/ franchisees are required to strictly adhere to the RBI AML/CFT guidelines applicable to money changing activities (RBI Master Direction on Money Changing Activities, s.3, para 9). Authorised dealers in foreign exchange are expected to put in place adequate arrangements for reporting of transactions by the agents/ franchisees to them on a regular basis (at least monthly) (s.3, para.7). They are also required to conduct regular spot audits of all locations of franchisees, at least once in six months) (s.3, para.7). A system of annual inspection of the books of the agents/franchisees should also be put in place to ensure that the money changing business is being carried out by the agents/franchisees in conformity with the terms of the agreement and prevailing RBI guidelines and that necessary records are being maintained by the agents/ franchisees) (s.3, para.8). Whilst authorized dealers in foreign exchange are required to monitor their agents as well as impart training to the franchisees/agents as regards operations and maintenance of records (s.3, Para 7).

*MTSS:* Overseas Principals are fully accountable for the actions of their agents and sub agents in India (Master Direction on MTSS, para 4(j)). However, there is no requirement for Overseas Principals that use agents to include them in their AML/CFT programmes and monitor them for compliance with these programmes.

Indian agents are required to conduct DD before appointing any sub-agents, are fully responsible for their sub-agents' activities, and any irregularity observed could render the Indian agent's permission liable for cancellation (para. 5.7). Indian agents and their sub-agents are subject to '*mutatis mutandis*' the RBI's Master Direction on KYC (Para 8, Master Direction on MTSS) in respect of cross-border inward remittance activities.

### *Weighting and Conclusion*

MVTS providers are licensed or registered by RBI and are monitored for AML/CFT compliance. Agents for MVTS providers are obliged entities for AML/CFT and need to be registered or the included in a list by the MVTS. There are, however, no specific requirements for MVTS providers to include their agents in their AML/CFT programmes.

**Recommendation 14 is rated Largely Compliant.**

## Recommendation 15 – New technologies

In its last MER, India was rated largely compliant with the requirements of former R.8, because there were inadequate provisions in the IRDA circulars to address the issues of technological developments and non-face-to-face business.

***Criterion 15.1 –*** At country level, India assesses from time-to-time ML/TF risks in relation to new products and new business practices. This is done in the ambit of the Joint Working Group (JWG)[163] and other contributing bodies[164]. The JWG is the central body responsible for coordinating the NRA process and includes all FI regulators. The JWG's Virtual Asset Contact Subgroup meets periodically (at least once a month) to discuss emerging risks from new products based on blockchain technology. FI Regulators' input in the process by sharing inputs from FIs or from the testing of new products in regulatory sandboxes[165].

At FI level, the PML Rules requires every FI to carry out a risk assessment to identify, assess and take effective measures to mitigate its ML/TF risks for clients, countries or geographic areas, and products, services, transactions or delivery channels that is consistent with the NRA (PML Rule 9(13)(i)). FIs are required to consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied ((Rule 9(13)(ii)(b)).

***Criterion 15.2 –***

a) FIs are required to undertake risk assessments prior to the launch or use of new products, practices and technologies (RBI's Master Direction on KYC, para. 62; SEBI Master Circular on AML/CFT, para.24A; IFSCA Guidelines on AML/CFT, para. 3.2; IRDAI's Master Guidelines on AML/CFT, para. 15.1; PFRDA's Guidelines on AML/CFT, para.9.6.2).

b) FIs in the securities, insurance and pension sectors and in the IFSC are required to take appropriate measures to manage and mitigate the risks (SEBI Master Circular on AML/CFT, para.24A; IFSCA Guidelines on AML/CFT, para. 3.2, IRDAI's Master Guidelines on AML/CFT, para. 15.1; PFRDA's Guidelines on AML/CFT, para.9.6.2). Banks and other FIs regulated by the RBI are required to ensure the adoption of an RBA to manage and mitigate the risks through appropriate EDD measures and transaction monitoring.

***Criterion 15.3 –***

a) India has carried out a sectoral risk assessment (SRA) of VAs and VASPs to identify and assess the ML/TF risks emerging from VAs and the activities or operations of VASPs, covering all VASP activities described in the FATF Glossary. The SRA was issued in February 2023, which was before India regulated the activity of VASPs and submitted them to registration.

[163] JWG comprises of representatives from MOF, MHA, FIU-IND, ED, CBI, NIA, IB, DRI, SFIO, NCB, CEIB, RBI, SEBI, IRDAI and other stakeholders.

[164] This includes the Indian Cyber Crime Coordination Centre and its National Cybercrime Threat Analytics Unit, which is a platform for LEAs, private sector, academia, and research organisations to work collaboratively in relation to cybercrime.

[165] The Enabling Framework for Regulatory Sandbox was published by RBI on 13 August 2019, with the purpose of live testing of new products or services in a controlled/test regulatory environment. Further, to facilitate testing of hybrid products/ services that straddle across the regulatory ambit of more than one FI regulator, a Standard Operating Procedure for Interoperable Regulatory Sandbox has been adopted.

Considering the fast-paced developments in the sector following the conclusion of the SRA, including India's decision to submit the sector to registration, the SRA is already outdated. India plans to review the SRA on an annual basis.

However, India continues to identify and assess ML and TF risks arising from VAs and VASPs through other means. Risk understanding is being informed by the VASP supervisor, FIU-IND regular engagement with LEAs in the monthly meetings of the virtual assets contact group, and through meetings of the sub-working group on P2P transactions and cybercrimes which is attended by VASPs and other FIs. Some insights on risks are also identified via supervisory activities.

a) VASPs are REs and subject to the requirements of the PMLA/PML Rules (MOF Notification of 7 March 2023). Under the provisions of PML Rules, FIU-IND has issued guidelines for AML/CFT compliance. The framework ensures that measures to prevent or mitigate ML and TF are commensurate with the risks identified.

b) VASPs are required to take the necessary steps to identify, assess, manage and mitigate their ML and TF risks, as required by c.1.10 and c.1.11 (PML Rule (13)(1); VASPs AML/CFT Guidelines, paras. 10, 5.2 and 5.3; MOF Notification dated 1 July 2005, ss.9(13) and 14(iii)).

***Criterion 15.4 –***

a) Persons that carry out the following activities for or on behalf of another natural or legal person in the course of business are REs (MOF Notification of 7 March 2023):

- exchange between virtual digital assets and fiat currencies;
- exchange between one or more forms of virtual digital assets;
- transfer of virtual digital assets;
- safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets; and
- participation in and provision of financial services related to an issuer's offer and sale of a virtual digital asset.

Virtual digital assets are defined as (Income Tax Act, s.2(47A)):

- any information or code or number or token (not being Indian currency or foreign currency), generated through cryptographic means or otherwise, by whatever name called, providing a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment scheme; and can be transferred, stored or traded electronically;
- a non-fungible token or any other token of similar nature, by whatever name called;
- any other digital asset as specified by Indian central government.

(i) The MOF and FIU-IND notifications are activity based. Any person including a legal person providing the listed services from India are

subject to registration requirements and this would include VASPs that are legal persons created in India.

(ii) Natural persons carrying out a 'VASP activity' (see above) from India are required to register in India (MOF Notification of 7 March 2023).

b) Pursuant to Standard Operating Procedure (SOP) for Registration of VASPs, following the electronic request for registration at FIU-IND's portal, FIU-IND organises an in-person meeting with the VASP proposed Designated Director and Principal Officer to understand the VASP business model, as well as their level of understanding of compliance requirements.

In addition, the VASP is required to furnish documentation related to (i) corporate structure and beneficial ownership of the company/entity. (ii) the entity incorporation, registration and annual financial statements (iii) details of business relationship with other entities along with copies of contracts (iv) a self-declaration to the effect that no proceedings have been initiated or are pending with ED or any other LEA against the applicant company/LLP or its directors/partners and no criminal cases are initiated/pending against the applicant company/LLP or its directors/partners (SOP for Registration of VASPs, FIU-IND Circulars of 17 October 2023 and 4 July 2023). There are no express provisions for checks to identify criminal associates and to prevent criminals or their associates from being a beneficial owner of a VASP; however, there is a general provision noting "background or antecedent verifications through various databases/sources of information" (SOP, para.2.2.3) would be conducted. Checks are performed with access to multiple databases such as the National Crime Records Bureau and CEIB.

***Criterion 15.5 –*** FIU-IND, LEAs, tax authorities and Indian Cyber Crime Coordination Centre (I4C) take action to identify legal persons that carry out VASP activities without the requisite licence or registration. FIU-IND uses market intelligence, social media and public source scraping to identify unregistered VASPs. So far it has detected 11 unregistered VASPs which were approached for registration, 7 of which are fully registered and the remaining 4 are undergoing registration. LEAs have also identified unregistered three VASPs and were reported to FIU-IND. Since then, these VASPs also complied with registration requirements.

FIU-IND can impose the sanctions specified in s.13 of the PMLA to unregistered VASPs (see c.15.8 below). In addition, the FIU-IND can request India's Ministry of Electronics and Information Technology to block the URLs of persons carrying out VASP activities without registration (pursuant to the Information Technology Act, s.69A).

***Criterion 15.6 –***

a) VASPs are subject to regulation and systems for monitoring and ensuring compliance with AML/CFT requirements (PMLA, s.54, PML Rules, 9(13)(14)). The supervisory authority, FIU-IND, conducts risk-based supervision of VASPs, which have been categorised based on their ML/TF risks according to SOPs and a risk-matrix developed by FIU-IND.

The supervision SOP defines the level of engagement with each category following a risk-based approach (annual offsite/onsite inspections and biannual review meetings for high-risk VASPs; biennial inspections and annual review meetings for medium-risk VASPs, and inspections every three years and review meetings every two years for low-risk VASPs).

However, no evidence was provided that FIU-IND needs to review its VASPs risk profiles periodically or when major events occur, or what these are.

b) FIU-IND has adequate powers to supervise and ensure compliance by VASPs with requirements to combat ML/TF, by conducting inspections, compelling the production of information and impose a range of disciplinary and financial sanctions, among others (PMLA, ss. 13 and 50; see also R.27). FIU-IND can deny or cancel registrations of VASPs that fail to comply with the provisions of the PMLA (FIU-IND Circular of 17 October 2023).

***Criterion 15.7 –*** India issued the AML/CFT Guidelines to VASPs, to assist this sector applying national AML/CFT measures, and, in particular, detecting and reporting suspicious transactions.

FIU-IND also provided feedback, which assisted VASPs in applying national measures to combat ML/TF. A feedback session was conducted on 25 May 2023 to newly onboarded VASPs on general and specific obligations, including reporting obligations, NRA findings and, monitoring of transactions and periodic risk assessment.

***Criterion 15.8 –***

a) The Director of FIU-IND may impose a series of a range of sanctions, including monetary sanctions (PMLA, s.13(2)) if VASPs fail to observe the record-keeping requirements (PMLA, s.12) or to provide the Director of FIU-IND with access to information (PMLA, s12A) that he or she considers necessary for the purposes of the PMLA. Monetary sanctions range from INR 10 000 (EUR 111) to INR 100 000 (EUR 1113) for each failure.

These sanctions are proportionate as they would directly correlate to the number of instances of violations identified and may be calibrated depending on the gravity of the violations and cover different AML/CFT obligations VASPs are subject to, including record-keeping requirements, enhanced due diligence, access to information by the Director of the FIU (under sections 12, 12A and 12AA in the PMLA), producing a risk assessment and having internal controls/ audit (Rule 9(13) of the PML Rules). However, these sanctions may not always be dissuasive, in particular for larger institutions or depending on the type of infraction. The FIU Director can also cancel the registration of VASPs not fulfilling their PMLA obligations.

In addition, the FIU-IND can request India's Ministry of Electronics and Information Technology to block the URLs of persons carrying out VASP activities without registration (pursuant to the Information Technology Act, s.69A).

For TFS, where there is indication of sufficient knowledge or participation into violation of TFS, the UAPA penalties would apply which are proportionate and dissuasive. However, as noted under R.6 and R.7, it is not clear to what extent VASPs can be administratively sanctioned for breaches of TFS obligations.

b) The sanctions established under the PMLA are applicable both to VASPs and designated directors or employees, where in the course of any inquiry, the Director finds that a RE or its designated director or any of its employees has failed to comply with CDD and other obligations imposed (PMLA, s.13(2)).

***Criterion 15.9 –*** VASPs are subject to the requirements specified in the PMLA/ PML Rules in the same manner as FIs, as set out in R.10 to 21, and are subject to the same shortcomings.

a) (India requires VASPs to conduct CDD in occasional transactions of INR 50 000 (EUR 563) or more (PML Rule 9(1)(b)(i)).

b) VASPs are subject to travel rule requirements (CERT-IN Directions[166] of 28 April 2022 by and VASP AML & CFT Guidelines, para. 11.3) in accordance with R.16:

- originating VASPs are required to obtain and hold accurate originator information and required beneficiary information on VA transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities.
- beneficiary VASPs are required to obtain and hold required originator information and accurate beneficiary information on VA transfers and make it available on request to appropriate authorities. This is applied regardless of whether the value of the VA transfer is denominated in fiat currency or another VA.
- VASPs are required to monitor wire transfers to detect those which lack the required originator and/or beneficiary information and screen the transactions to comply with relevant UNSCR resolutions.

There are no specific provisions requiring that the same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer, as required under c.15.9 (iv). However, FIs in India have not been given license or authorisation to send or receive virtual assets.

***Criterion 15.10 –***

The obligations under s51 UAPA and s12A of the WMD Act and the TFS framework based on the relevant OMs thereunder (see R.6 and 7) apply to VASPs. FIU-IND also provides updates to the TF and PF TFS lists which are forwarded to the Reporting Entities registered with FIU-IND through FINNET.

***Criterion 15.11 –***

A wide range of international cooperation may be provided to countries relating to VASPs, pursuant to sections 58, 58A, 58B and 60 of the PMLA.

FIU-IND may exchange information with foreign FIUs through the Egmont Group, and foreign LEAs through informal international co-operation, in the sense of R.40.

India has not demonstrated that FIU-IND is able to exchange information with foreign supervisors (in their capacity as a supervisor) on VASP related matters.

## *Weighting and Conclusion*

India has assessed the risks related to new technologies and there are requirements for FIs to undertake risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks.

On virtual assets and VASPs, India introduced a registration regime in March 2023 and all VASPs are subject to AML/CFT obligations. The VASP SRA, carried out before the incorporation of the sector to AML/CFT obligations, is somewhat outdated and limited in scope. There are requirements to prevent criminals from owning or controlling or hold a management function in a VASP, but they do expressly not provide for checks to identify criminal associates and to prevent criminals or their associates from being a beneficial owner of a VASP. VASPs are subject

[166] The directions were issued by the Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics & Information Technology.

to risk-based AML/CFT supervision. Sanctions may not be sufficiently dissuasive for larger businesses. Guidance provided to the sector is adequate and India brought in requirements to implement the travel rule. India has not yet established channels for international cooperation with other VASP supervisors.

**Recommendation 15 is rated Largely Compliant.**

## Recommendation 16 – Wire transfers

In its last MER, India was rated largely compliant with the requirements of former SRVII, because the PMLA did not apply to India Post, which is authorised to conduct both domestic and cross border wire transfers until June 2009.

***Criterion 16.1*** – FIs regulated by the RBI are required to ensure that all cross-border wire transfers are accompanied by accurate[167], complete, and meaningful originator and beneficiary information, including (RBI's Master Direction on KYC, para. 64(A)(i)):

a) (i) name of the originator; (ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction; (iii) the originator's address, or national identity number, or customer identification number, or date and place of birth;

b) (i) name of the beneficiary; and (ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

FIs regulated by IFSCA are required to ensure that all cross-border wire transfers of USD 1 000 or more include all requirements listed above (IFSCA's Guidelines on AML/CFT, paras. 7.7.2, 7.7.3).

***Criterion 16.2*** – For FIs regulated by the RBI, batch transfers, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the individual transfers are required to include the originator's account number or unique transaction reference number, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country (RBI's Master Direction on KYC, para. 64(A)(ii)).

Banks regulated by IFSCA are subject to all requirements of this criterion (as above for FIs regulated by the RBI) with respect to cross-border wire transfers of USD 1000 or more, including transfers which are bundled in a batch file (IFSCA's Guidelines on AML/CFT, para.7.7.3(b), IFSCA Circular-Additional AML Measures).

***Criterion 16.3*** – For FIs regulated by the RBI, there is no *de minimis* threshold and the requirements noted under c.16.1 equally apply to transactions below USD 1 000. FIs regulated by IFSCA are required to include for transactions equal or below USD 1 000, (i) the name of the wire transfer originator; (ii) the wire transfer originator's account number (or unique transaction reference number where no account number exists); (iii) the name of the wire transfer beneficiary; and (iv) the wire transfer beneficiary's account number (or unique transaction reference number where no account number exists) (IFSCA's Guidelines on AML/CFT, para. 7.7.2).

[167] FIs are required to verify identity while carrying out any international money transfer operations (PML Rule 9(1)(b)(ii)).

***Criterion 16.4 –*** For FIs regulated by the RBI, there is no *de minimis* threshold and the requirements noted under c.16.1 equally apply to transactions below USD 1 000.

Banks regulated by the IFSCA are required to verify the information pertaining to its customer, where there is a suspicion of ML/TF (IFSCA's Guidelines on AML/CFT, para7.2A).

***Criterion 16.5 –*** In relation to domestic wire transfers, FIs regulated by the RBI are required to ensure that the information accompanying the wire transfer includes originator information for wire transfers equal or above INR 50 000 (EUR 558) or when the originator is an account holder of the ordering FI (RBI's Master Direction on KYC, para. 64(A)(iii)(iv)). For domestic wire transfers below INR 50 000, where the originator is not an account holder of the ordering FI and where the information accompanying the wire transfer can be made available to the beneficiary FI and appropriate authorities by other means, it is sufficient for the ordering FI to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary (RBI's Master Direction on KYC, para. 64(A)(iv)).

FIs regulated by the IFSCA are required to ensure that the information accompanying wire transfer includes originator information as indicated for cross-border wire transfers; *or alternatively* only the wire transfer originator's account number (or unique transaction reference number where no account number exists), provided: (i) that these details will permit the transaction to be traced back to the wire transfer originator and wire transfer beneficiary; the ordering institution shall provide the wire transfer originator information under the terms specified in the IFSCA's Guidelines on AML/CFT (para. 7.7.4) (see c.16.6 below).

***Criterion 16.6 –*** Ordering FIs regulated by the RBI are required to include, in the circumstances referred in c.16.5, full originator and beneficiary information on all domestic wire transfers equal or above INR 50 000 (EUR 558) (see c.16.5 above), and therefore this criterion does not apply to them. In relation domestic wire transfers below INR 50 000, the ordering FIs are required to make available the account number of a unique transaction reference number that allows tracing of the originator or beneficiary within three working/business days of receiving the request from the intermediary FI, beneficiary FI, or from appropriate competent authorities (RBI's Master Direction on KYC, para. 64(A)(iv)).

RBI-regulated FIs are required to ensure that all the information on the wire transfers is immediately made available to appropriate law enforcement and/or prosecutorial authorities as well as FIU-IND on receiving such requests with appropriate legal provisions (RBI's Master Direction on KYC, para. 64(A)(v)).

Ordering FIs are required to, in the circumstances referred in c.16.5, provide the wire transfer originator information: (i) within three business days of a request for such information by the beneficiary institution, by the IFSCA or other relevant authorities; and (ii) immediately upon request for such information by law enforcement authorities in India (IFSCA's Guidelines on AML/CFT, para. 7.7.4 (b)).

***Criterion 16.7 –*** All FIs are required to maintain records of all transactions, for a period of five years from the date of transaction between a client and the FI (PMLA, s.12). FIs regulated by the RBI are required to preserve complete originator and beneficiary information for at least five years from the date of transaction (RBI's Master Direction on KYC, s.64 and s.46). Ordering FIs regulated by IFSCA are required to record adequate details of the wire transfer (IFSCA's Guidelines on AML/CFT, s.7.7) and preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended (s.9.1(g) and 9.2).

***Criterion 16.8*** – Ordering FIs regulated by the RBI and IFSCA are not allowed to execute the wire transfer if they do not comply with the requirements set out in c.16.1-16.7 (RBI's Master Direction on KYC, para.64(B)(i)(c) and IFSCA's Guidelines on AML/CFT, para. 4.7.4 (c)).

***Criterion 16.9*** – FIs regulated by RBI and IFSCA are required, in respect of cross border transfers, when acting as an intermediary institution to ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it (RBI's Master Direction on KYC, para.64(B)(ii)(a); IFSCA's Guidelines on AML/CFT; para 7.7.6 (a)).

***Criterion 16.10*** – Intermediary FIs are required to, where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, keep a record, for at least five years, of all the information received from the ordering FI or another intermediary FI (RBI's Master Direction on KYC, para.64(B)(ii)(b); IFSCA's Guidelines on AML/CFT; Para 7.7.6(b)).

***Criterion 16.11*** – Intermediary FIs regulated by RBI and IFSCA are required to take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information; such measures should be consistent with straight-through processing (RBI's Master Direction on KYC, para.64(B)(ii)(c); IFSCA's Guidelines on AML/CFT, para 7.7.6(c)).

***Criterion 16.12*** – Intermediary FIs regulated by RBI and IFSCA are required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action (RBI's Master Direction on KYC, para.64(B)(ii)(d); IFSCA's Guidelines on AML/CFT, para. 7.7.6(c)).

***Criterion 16.13*** – Beneficiary FIs regulated by RBI and IFSCA are required to take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information (RBI's Master Direction on KYC, para.64(B)(iii)(a); IFSCA's Guidelines on AML/CFT, para. 7.7.5(a)).

***Criterion 16.14*** – For cross-border wire transfers, beneficiary FIs regulated by the IFSCA are required to identify and verify the identity of the wire transfer beneficiary if the identity has not been previously verified (IFSCA's Guidelines on AML/CFT; Para 7.7.5(b)) and maintain this information in accordance with R.11.

For FIs regulated by the RBI, there is no *de minimis* threshold and the requirements noted under c.16.1 equally apply to transactions below USD 1 000. RBI regulated FIs are required to undertake identification of customers when carrying out any international money transfer operations for a person who is not an account holder of the RE (RBI's Master Direction on KYC, para.13(b)). For beneficiaries who are accountholders, FIs would have already verified the identity of the customer when opening the account (PML Rule 9(1)(a)). They are also required to maintain all information in accordance with R.11.

***Criterion 16.15*** – Beneficiary FIs regulated by RBI and IFSCA are required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action (RBI's Master Direction on KYC, para.64(B)(iii)(b); IFSCA's Guidelines on AML/CFT, para. 7.7.5(c)).

***Criterion 16.16*** – Some MVTS providers (MTSS, PPI issuers) are required to comply with all of the relevant requirements of R.16, whether they are providing services directly or through their agents (RBI's Master Direction on KYC, para 64 (B)(iv), Master Direction on MTSS (para.8), Master Direction on PPIs (para.6)).

***Criterion 16.17 –*** In cases where a MVTS provider controls both sides of a wire transfer (RBI Master Direction on KYC, s.64(B)(iv)):

a) The MVTS provider is required to take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

b) The MVTS provider is required file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

***Criterion 16.18 –*** When undertaking cross-border wire transfer, FIs regulated by the RBI are prohibited from conducting transactions with designated persons and entities and to ensure that they do not process cross-border transactions of designated persons and entities (RBI's Master Direction on KYC, para.64(C)(ii)) and take freezing actions (para.51(c), para 52(a)).

FIs in the IFSC are required to, where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or a terrorist entity, block, reject or freeze assets of these terrorists or terrorist entities immediately (IFSCA's Guidelines on AML/CFT, para. 7.4).

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 16 is rated compliant.**

## Recommendation 17 – Reliance on third parties

The last MER of India considered that former R.9 was not applicable, because third-party introduced business was not permitted.

**Criterion 17.1 –** FIs are permitted to rely on third parties to perform elements (a)-(c) of the CDD measures set out in R.10 and are ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable (PML Rule 9(2)(e)).

a) FIs are required to immediately obtain from the third party or from the Central KYC Registry records or information of the CDD carried out by the third party immediately (PML Rule 9(2)(a)).

b) FIs are required to take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirement will be made available from the third party upon request without delay (PML Rule 9(2)(b)).

c) FIs are required to satisfy themselves that a third party is regulated, supervised, or monitored, and has measures in place for compliance with CDD and record-keeping requirements (Rule 9(2)(c)).

***Criterion 17.2 –*** FIs must satisfy themselves that the third party is not based in a country or jurisdiction assessed as high risk (PML Rule 9(2)(d)). Authorities indicated that the FATF's assessment would be basis for assessing a jurisdiction as high risk. However, the requirement does not fully align with the standards, which require the FI to have regard to information available on the level of country risk (which is broader than just high risk) when determining in which countries the third party can be based.

***Criterion 17.3 –*** Except for the *IFSC*, FIs that rely on third parties in the same financial group are subject to the same requirements as under 17.1.

The *IFSC* regulator provided for alternative requirements (as permitted under PML Rule 9(2)(f)). IFSC FIs can rely on member of the financial group if (i) the financial group applies and implements a group-wide policy on CDD and record keeping, which meets the standards set out in the FATF Recommendations 10 to 12; and (ii) the implementation of CDD and record keeping at the group level are supervised by a financial services regulator or other competent authority in a country. Moreover, the relied third party cannot be based in a country or jurisdiction assessed as high risk (IFSCA's Guidelines on AML/CFT; para. 6.2).

### *Weighting and Conclusion*

There is a minor deficiency in relation to criterion 17.2, and, while FIs are required to satisfy themselves that the third party is not based in a country or jurisdiction assessed as high risk, this is not equivalent to the standard, which requires the FI to have regard to information available on the level of country risk (which is broader than just high risk) when determining in which countries the third party can be based.

**Recommendation 17 is rated Largely Compliant.**

## Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its last MER, India was rated largely compliant with former R.15 and compliant with former R.22. Shortcomings related to the role of the principal officer in the banking sector (except for authorised money changers) being restricted to STR and other reporting, and not extending to overall compliance; and the lack of an express requirement for the audit function in the securities sector be adequately resourced, and a resource issue to be addressed in the insurance sector.

***Criterion 18.1*** **–** FIs are required to implement a CDD programme which have regard to the ML and TF risks and the size of the business and include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the reporting entity or through national risk assessment (PML Rule 9(13)(ii)(iii)). In addition, FIs are required to:

a) communicate to the Director of FIU-IND the name, designation and address of the Principal Office, who is defined as an officer at management level designated by the FI (Rule 7(1), Rule 2(1)(f)).

b) put in place adequate screening mechanism as an integral part of their personnel recruitment/hiring process.[168]

c) put in place on-going employee training programmes so that the members of staff are adequately trained in KYC and more generally in the FI AML/CFT policies and procedures.[169]

[168] RBI's Master Direction on KYC (para.70(a)), SEBI's Master Circular on AML/CFT (para.65), IRDAI's Master Guidelines on AML/CFT (para. 6.1), PFRDA's Guidelines on AML/CFT (para. 6.1), IFSCA's Guidelines on AML/CFT, s.12.1(a)(i).

[169] RBI's Master Direction on KYC (para.70(c)), SEBI's Master Circular on AML/CFT (para.66), IRDAI's Master Guidelines on AML/CFT (para. 6.2), PFRDA's Guidelines on AML/CFT (para. 6.2), IFSCA's Guidelines on AML/CFT (para 8.4).

d) have an independent internal audit system to verify the compliance with the FI's AML/CFT policies and procedures.[170]

***Criterion 18.2 –*** Financial groups are required to implement group-wide policies for the purpose of discharging their obligations under PMLA (PML Rules, Rule 3A(2)). Groups are defined as a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes,— (i) is required to be prepared under the laws of the country or territory of which the parent entity is resident; or (ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident (PML Rules, Rule 2(cba); Income Tax Act, 1961, s.286(9)(e)).

Moreover, the following specific requirements apply:

a) Every RE which is part of a group is required to implement group-wide programmes against ML and TF, including group-wide policies for sharing information required for the purposes of CDD and ML and TF risk management (PML Rule 3A(1); Regulators directions, e.g., RBI Master Direction on KYC, para.4(b));

b) There are no specific requirements for the provision, at group-wide level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information in respect of FIs in the banking/ MVTS sector (i.e., FIs regulated by RBI). FIs in the *IFSC*, as well as in the securities, insurance and pension sectors are required to provide at group-wide compliance, audit and AML/CFT functions of customer, account, and transaction information from its branches and subsidiaries, when necessary for the purposes of ML/TF risk management (IFSCA's Guidelines on AML/CFT, para.12.2(e); SEBI Master Circular on AML/CFT, para 7B, IRDAI Master Guidelines on AML/CFT, para 4.6, PFRDA Master Guidelines on AML/CFT, para 4.4.4). For FIs in the securities, insurance and pension sectors, there is a specific requirement for including information and analysis of transactions or activities which appear unusual (if such analysis was done), but such a requirement is not provided for the IFSC FIs.

c) For all REs, there is a requirement for the group-wide programmes to include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off (PML Rule 3A(1)).

***Criterion 18.3 –*** Banks and other FIs regulated by the RBI are required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with RBI Master Directions on KYC, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit this. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, FIs are required to inform the RBI, which may advise further necessary action by the FI including application of additional measures to be taken by the FI to manage the ML/TF risks (RBI Master Direction on KYC, para 2(b)(i)).

[170] RBI's Master Direction on KYC (para. 8(a)(iii), (iv) & (v)), RBI's Circular of 7 January 2021 on Risk Based Internal Audit Framework, SEBI's Master Circular on AML/CFT (para. 9 (vi) & (vii)), IRDAI's Master Guidelines on AML/CFT (para. 4.3.6 and para. 7), PFRDA's Guidelines on AML/CFT (para. 4.3.6 and para. 7), IFSCA's Guidelines on AML/CFT (para 8.3).

In relation to the securities, insurance and the IFSC, branches/overseas subsidiaries of registered FIs are required to, in case of variance in CDD/ AML standards specified by the Indian regulator and the regulators of the host country, to adopt the more stringent requirements of the two. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups are required to apply appropriate additional measures to manage the ML/TF risks, and inform the Indian regulator (SEBI's Master Circular on AML/CFT, para.6, IRDAI Master Guidelines on AML/CFT, para 2.2A, IFSCA, Guidelines on AML/CFT, para.12.2(c) and (d)).

For the pension sector, the overseas branches of the FI are required to conduct CDD following PFRDA requirements for pension schemes regulated/administered by PFRDA. If the host country does not permit implementation of the PFRDA guidelines, the FI should apply appropriate additional measures to manage the money laundering and terrorist financing risks and inform the same to PFRDA (PFRDA Master Guidelines on AML/CFT, para 4.4.5).

### *Weighting and Conclusion*

FIs are required to develop and implement programmes against ML/TF and are required to implement internal policies at the group level, including on data protection and information sharing within the group. However, there are no specific requirements for the provision, at group-wide level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information in respect of FIs in the banking/ MVTS sector (except in relation to the IFSC).

**Recommendation 18 is rated Largely Compliant.**

## Recommendation 19 – Higher-risk countries

In its last MER, India was rated partially compliant with former R.21. The following shortcomings were noted: (i) the PMLA did not apply to commodities futures brokers; (ii) there was no clear and direct requirements for FIs 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; (iii) FIs were not expressly required to examine the background and purpose of transactions with persons from or in these countries; (iv) India had no clear legal authority that enabled it to apply a range of appropriate counter-measures in the securities or insurance sectors; and (v) There was an effectiveness concern, that FIs did not look beyond the FATF statements, and made little use of publicly available information when identifying countries which did not or insufficiently apply the FATF Recommendations. The 8th FUR of India concluded that India had addressed some technical deficiencies and that its level of technical compliance with former R.21 was essentially equivalent to LC.

***Criterion 19.1 –*** All FIs to conduct EDD prior to the commencement of specific transactions, including a transaction or class of transactions where there is a high ML or TF risk (PMLA, s.12AA). More specific requirements are set by the FI Regulators:

a) *Banks, NBFCs and MVTS*: FIs are required to give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements (RBI's Master Direction on KYC, para.56), or that FATF Public Statement, may also be used in risk assessment (para. 12).

b) *Other FIs:* Securities intermediaries, insurers and *IFSC* FIs are required to apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions)

from countries for which this is called for by the FATF (SEBI Master Circular on AML/CFT, para 12(iii)(f), IRDAI Master Guidelines on AML/CFT, para 17.1; IFSCA Guidelines on AML/CFT, para 5.6(c)). For the pension sector, the requirement refers to business relationships and transactions with individuals only (PFRDA Master Guidelines on AML/CFT, para 16.1, para.2(e)).

***Criterion 19.2 –*** The PML Rules provide that the Regulators guidelines shall include countermeasures to be undertaken when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government (PML Rule (9(14)(ib)). Regulators have established the following requirements:

a) Banks, NBFC and MVTS: FIs are required to undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government (RBI's Master Direction on KYC, para 53B);

b) *Securities: Intermediaries a*re required to undertake EDD measures to Clients of Special Category including clients in high-risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as identified by the FATF. Registered intermediaries are directed that such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying EDD while expanding business relationships with the identified country or persons in that country etc. (SEBI's Master Circular on AML/CFT para 35, para. 12(ii));

c) *Insurance*: FIs are required to apply countermeasures proportionate to the risk when called for by FATF. To go beyond FATF statements and consider publicly available information and to take cognizance of vulnerabilities shared by government of India, and the regulator in ML/TF risk assessments (IRDAI Master Guidelines on AML/CFT, para. 17.1 and para 9.1);

d) *Pension*: FIs are required to apply EDD measures, proportionate to the risks, to business relationships and transactions with individual from countries for which this is called for by the FATF (PFRDA Master Guidelines on AML/CFT, para 16.1);

e) *IFSC*: FIs are required to apply EDD measures depending upon the risk profile of the customer to be decided on case-to-case basis. Circumstances where a customer presents or may present a high probability of ML/TF risk may include (i) where a customer or any BO of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures; and (ii) where a customer or any BO of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the FI for itself or notified to Regulated Entity generally by IFSCA or other relevant domestic authorities in India or other foreign regulatory authorities (IFSCA Guidelines on AML/CFT, para 5.6).

The measures set to the securities, pension and the IFSC do not fully address the criterion as they are limited to EDD.

***Criterion 19.3 –*** India has put in place measures to ensure that FIs are informed of concerns about the deficiencies of other countries' AML/CFT systems, including the issuing of circulars by regulators to the FIs to inform them of the weakness in the AML/CFT system. The regulators do

this under the general power to issue directions to the FIs (RBI's Master Direction on KYC, para 54; SEBI Master Circular on AML/CFT para 12(f)). Further, RBI issues a press release after each FATF plenary regarding the FATF public statements as and when advised by the Government of India, and SEBI also disseminates FATF public statements in its website.

### *Weighting and Conclusion*

The regulations for the securities, pension and the IFSC fall short of a requirement to be able to apply countermeasures proportionate to risks, as required under c.19.2.

**Recommendation 19 is rated Largely Compliant.**

## Recommendation 20 – Reporting of suspicious transactions

In its last MER, India was rated partially compliant with the former R.13 and SR.IV. Deficiencies related to the following: the PMLA did not apply to commodities futures brokers; there was 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; there were concerns about the low number of STRs filed in relation to ML and FT (especially in relation to the banking sector). The 8th FUR of India concluded that India's level of technical compliance with former R.13 and SR.IV was essentially equivalent to LC.

***Criterion 20.1 –*** Pursuant to the PMLA, FIs are legally required to provide to the Director of FIU-IND, within such time as may be prescribed, information relating to transactions, whether attempted or executed, the nature and value of which may be prescribed (PMLA, s.12(1)(b)). The Central Government is empowered to make rules in relation to the referenced provision, prescribing the nature and value of transactions and the time within which they are to be reported (PMLA, s.73(2)(i)). The PML Rules, drafted under section 73 of the PMLA, require the Principal Officer of a FI, after being satisfied that transactions specified in Rule 3(1)(D) of the PML Rules are suspicious (see more below in c.20.2), to submit information promptly to the Director of FIU-IND in respect of such transactions (PML Rule 8(2)). The Rules are enforceable as the PMLA clearly specifies that further aspects will be prescribed by the central government.

***Criterion 20.2 –*** A "suspicious transaction" is defined in the PML Rules (Rule 2(1)(g)) as a transaction, including an attempted transaction, whether or not made in cash, which in the view of a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the PMLA, regardless of the value involved; or

b) appears to be made in circumstances of unusual or unjustified complexity; or

c) *appears* to have no economic rationale or *bonafide* purpose; or

d) *gives* rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.

As noted in c.20.1 above, the Principal Officer of a FI is required to report the transactions referred in Rule 3(1)(D) of the PML Rules after being satisfied that they are suspicious (PML Rule 8(2)). Rule 3(1)(D)[171] requires FIs to maintain a record of all transactions, including the record

[171] Rule 3 reads as follows: "Every reporting entity shall maintain a record of all transactions including the record of,— (…)
(D) all suspicious transactions whether or not made in cash and by way of:

of all suspicious transactions whether or not made in cash and by way of deposits and credits, withdrawals, wire transfers etc. Whist the list of transactions is comprehensive, it does not expressly cover all types of transactions that FIs carry out. India interprets considers that the list is not exhaustive and guidance issued by supervisors interprets the obligation to report STRs in line with the definition in Rule 2(1)(g) as mentioned above.

### *Weighting and Conclusion*

Reporting requirements are comprehensive. There is some ambiguity on whether the list of suspicious transactions is exhaustive or exemplificative, but guidance has clarified that reporting requirements should be interpret broadly and in line with the standard.

**India is rated Largely Compliant with Recommendation 20.**

## Recommendation 21 – Tipping-off and confidentiality

In its last MER, India was rated largely compliant with former R.14, because directors or employees were not expressly covered by the PMLA's safe harbour provision.

***Criterion 21.1* –** FIs, their directors and employees shall not be liable to any civil or criminal proceedings against them for providing information on transactions to the Director of FIU-IND (PMLA, s.14). However, the Director may still impose fines and other sanctions to FIs, their directors and employees for failures under the PMLA (PMLA, ss.13 and 14).

***Criterion 21.2* –** The PMLA contains a requirement for "information maintained, furnished or verified, save as otherwise provided under any law for the time being in force" be kept

(i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of : (a) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or (b) travellers cheques, or (c) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or (d) any other mode in whatsoever name it is referred to;

(ii). credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:— (a) payment orders, or (b) cashiers cheques, or (c) demand drafts, or (d) telegraphic or wire transfers or electronic remittances or transfers, or (e) internet transfers, or (f) Automated Clearing House remittances, or (g) lock box driven transfers or remittances, or (h) remittances for credit or loading to electronic cards, or (i) any other mode of money transfer by whatsoever name it is called;

(iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of: (a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or (b) purchase and negotiation of bills, cheques and other instruments, or (c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or (d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support; (v) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to."

confidential (s.12(2)). Moreover, the PML Rules requires every reporting entity, its directors, officers, and all employees to ensure that the maintenance of records of suspicious transactions and furnishing of information to the Director are kept confidential (PML Rule, 8(6)). FI Regulators' guidelines and directions note the prohibition to disclose STRs, that this prohibition extends to FI's directors, officers and employees and that this should not inhibit information sharing among group entities under R.18 (RBI's Master Direction on KYC, para. 49; SEBI's Master Circular on AML/CFT, para.60, IRDAI's Master Guidelines on AML/CFT, para. 18.4, PFRDA's Guidelines on AML/CFT, para. 17.5 and IFSCA's Guidelines on AML/CFT, para 10.4).

### *Weighting and Conclusion*

All criteria are met.

**India is rated Compliant with Recommendation 21.**

## Recommendation 22 – DNFBPs: Customer due diligence

In its last MER, India was rated non-compliant with the requirements of former R.12. CDD requirements did not apply to any of the DNFBP sectors, with the exception of casinos. For casinos, only the basic requirements of the PMLA and the accompanying rules applied to casinos, and these did not address much of the detail required under the FATF standards. Moreover, the extension of the PMLA to the casino sector was very recent and there was insufficient evidence of effective implementation. India's 8th FUR concluded that, although India had made progress with addressing some shortcomings, it could not be concluded that its level of compliance would be equivalent to largely compliant.

AML/CFT requirements for DNFBPs

The following DNFBPs are covered by AML/CFT requirements (PMLA, s. Section 2(sa); Notification S.O.2036(E) of 3 May 2023 and Notification S.O.2135(E) of 9 May 2023):

a) persons carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casinos;

b) real estate agents with a minimum annual turnover of INR 2 million (EUR 22 000)

c) dealers in precious metals, precious stones and other high value goods;

d) persons engaged in safekeeping and administration of cash and liquid securities on behalf of other persons;

e) persons, including Chartered Accountants, Company Secretaries, Cost and Works Accountants, carrying out on behalf of their client, in the course of their profession, the following activities:

- buying and selling of any immovable property;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of companies, LLPs or trusts, and buying and selling of business entities.

f) persons carrying on, in the course of business, on behalf of or for another person, the following activities:

- acting as a formation agent of companies and LLPs;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a firm or a similar position in relation to other companies and LLPs;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company or an LLP or a trust;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another type of trust; acting as (or arranging for another person to act as) a nominee shareholder for another person.

***Criterion 22.1 –*** DNFBPs in India are required to apply the CDD requirements set out in the PMLA and PML Rules as described in relation to R.10 (and are subject to the same technical deficiencies noted in R.10). The CDD requirements in the PMLA/ PML Rules requirements are supplemented by sector specific guidelines which provides details for understanding by the entities and do not introduce additional requirements to the entities beyond the PMLA and the PML Rules. The framework is further detailed below:

a) Casinos are required to verify the identity of all customers who engage in financial transactions which are equal to or exceeding INR 50 000 (EUR 548), whether conducted as a single transaction or several transactions that appear to be connected (PMLA, s.2(1)(sa)(i), s.2(1)(wa) and s.11A; PML Rule 9).

b) Real estate agents with a minimum annual turnover of INR 2 million (EUR 22 000) as per Notification G.S.R. 798(E) dated 28.12.2020 are required to conduct CDD when providing services in relation to sale or purchase of real estate. Whilst the exemption from of real estate agents with a turnover below the set threshold is based on a risk assessment for the sector, threats in the sector were not fully considered (see Recommendation 1, c.1.6).

c) DPMS are considered REs if they engage in any cash transactions with a customer equal to or above INR 1 million (EUR 11 035), carried out in a single operation or in several operations that appear to be linked (Notification G.S.R. 799(E) dated 28.12.2020, CBIC DPMS Guidelines, s.2.2). However, DPMS, as other persons in India, are currently prohibited from receiving cash payments of INR 200 000 (EUR 2 222) or more pursuant the Income Tax Act (s.269ST, s.271DA). As a result of the tax law provisions, DPMS are currently not able to perform cash transactions that would attract the application of CDD obligations set in the PMLA and the PMLA Rules (see Immediate Outcome 3, section 6.2.1 for more details).

d) Accountants (including Chartered Accountants and Cost Accountants) are subject to the CDD obligations specified under the PMLA/ PML Rules as described in R.10 when carrying on the specific activities listed in c.22.1.d (Notification S.O.2036(E) of 3 May 2023)).

Lawyer and notaries are subject to the PMLA and PML Rules when carrying prescribed activities in the notifications. However, persons carrying out on behalf of a client in the course of their profession the activities listed in c.22.1.d are considered REs. The activities permitted for

notaries to conduct in terms of the Notaries Act, 1952 (s.8) do not seem to fall within the category subject to c.22.1.

If the accountant or lawyer is only involved in the preparation for the activity listed in c.22.1.d of the Methodology (e.g., drafting by-laws of a company, sale and purchase agreement for a real estate transaction or reviewing an investment proposal), but does not then actually carry out the activity for their client, they are not considered are a RE pursuant to the Notification.

e) Any person carrying on, in the course of business, on behalf of or for another person, the services described in c.22.1.e is a RE (PMLA, s. Section 2(sa) and Notification S.O.2135(E) of 9 May 2023). Similarly, when the person is only involved in the preparation for the activity, there are no requirements in place.

***Criterion 22.2*** – DNFBPs are required to comply with the same record-keeping requirements as FIs under the PMLA and PML Rules– see analysis of R.11. However, as noted under c.21.1, (i) real estate agents with a turnover below the set threshold and (ii) accountants, lawyers and TCSPs when they are only involved the preparatory work are not considered REs.

***Criterion 22.3 –*** DNFBPs in India are required to comply with the same PEPs requirements as FIs under the PMLA/PML Rules and are subject to the same deficiencies identified, in particular for domestic PEPs– see analysis of R.12 and also scope gap identified in c.21.b), d) and e).

***Criterion 22.4 –*** DNFBPs in India are required to comply with the same new technologies requirements as FIs under the PMLA and PML Rules– see analysis of R.15. DNFBPs are required to carry out a risk assessment to identify, assess and take effective measures to mitigate its ML/TF risks for clients, countries or geographic areas, and products, services, transactions or delivery channels that is consistent with the NRA (PML Rule 9(13)(i)).

Guidelines for casinos and real estate agents[172] cover the requirements for undertaking risk assessments prior to the launch or use of such products, practices and technologies while no similar requirements for accountants, lawyers, and TCSPs are present. See also scope gap identified in c.21.b), d) and e).

***Criterion 22.5 –***

DNFBPs in India are required to comply with the same third-party reliance requirements as FIs under the PMLA/PML Rules and are subject to the same shortcomings in respect of c.17.2 – see analysis of R.17. See also scope gap identified in c.21.b), d) and e).

### *Weighting and Conclusion*

Real estate agents with a turnover below the set threshold as well as accountants, lawyers and TCSPs are not considered REs when they are only involved the preparatory work and that impacts all criteria. There is also moderate a shortcoming arising from not having legal requirements for DNFBPs to apply CDD measures in respect of domestic PEPs. For lawyers, accountants and TCSPs, there are no obligations for undertaking risk assessments prior to the launch or use of such products, practices and technologies. Other obligations are in place.

**Recommendation 22 is rated Largely Compliant.**

## Recommendation 23 – DNFBPs: Other measures

[172] Goa Casinos AML/CFT Guidelines, para 10(j); Sikkim Casinos AML/CFT Guidelines, para 9(i), REA AML/ CFT Guidelines, Para 5.2(vii).

In its previous MER, India was rated non-compliant with former R.16. A scope deficiency was noted as the PMLA did not apply to any of the DNFBP sectors, with the exception of casinos. In addition. for casinos, only the basic requirements of the PMLA and the accompanying rules applied, and these did not address much of the detail required under the FATF standards. Moreover, the extension of the PMLA to the casino sector was very recent and there was insufficient evidence of effective implementation. India's 8th FUR concluded that, although India had made progress in implementing former R.16, its level of compliance was not yet equivalent to largely compliant.

***Criterion 23.1* –** DNFBPs in India are subject to the same STR requirements as FIs and subject to the same shortcomings (as set out in R.20). Real estate agents with a turnover below the set threshold as accountants, lawyers and TCSPs are not considered REs when they are only involved the preparatory work, and therefore, are not required to submit a STR in relation (financial) transactions in relation to such activities. These shortcomings also impact the criteria below.

***Criterion 23.2* –** DNFBPs are required to comply with the same internal control requirements and group-wide measures established under the PMLA/PML Rules as FIs, and subject to the same shortcomings– see analysis of R.18.

There are no requirements for the provision, at group-wide level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information (see c.18.2(b)) and in relation to c.18.3 for DNFBPs.

***Criterion 23.3* –** DNFBPs are required to comply with the same higher-risk countries requirements established under the PMLA/PML Rules as FIs – see analysis of R.19. For real estate agents, there are additional EDD measures in para 6.4 of the Guidelines to cover transactions and business relationships emanating from high-risk jurisdictions. However, the shortcoming identified in c.19.2 equally applies to DNFBPs.

***Criterion 23.4*** – DNFBPs are required to comply with the same confidentiality requirements established under the PMLA and PML Rules as FIs – see analysis of R.21.

### *Weighting and Conclusion*

India has minor shortcomings for not fully having mitigating measures on the applicable Recommendations. Real estate agents with a turnover below the set threshold as well as accountants, lawyers and TCSPs are not considered REs when they are only involved the preparatory work, which impacts all relevant criteria.

**Recommendation 23 is rated Largely Compliant.**

## Recommendation 24 – Transparency and beneficial ownership of legal persons

In its last MER, India was rated partially compliant with the former R.33. Deficiencies included the availability of beneficial ownership (BO) information of legal persons beyond information on immediate owners, lack of measures to prevent the misuse of Hindu Undivided Family Businesses (HUFs) for ML/TF and no timely access to BO information by law enforcement and other authorities.

***Criterion 24.1* –** The two types of legal persons in India are companies and limited liability partnerships (LLPs). Their different forms, and basic features are set out in the Companies Act, 2003 (CA) and the Limited Liability Partnership Act, 2008 (LLPA), respectively.

- Companies are incorporated in accordance with the CA (ch.2) and can take the form of *private companies* (i.e., companies formed by one (One Person Company)

or more persons up to 200 and restrict the rights to transfer their shares) and *public companies* (which can formed by seven or more persons and are not "a private company") (CA, ss.2(68), 2(71), 3(1)). Companies (private or public) can be *limited by shares*, *limited by guarantee*, or *unlimited*. Also limited companies can also hold the status of non-profit organisations (CA, s.8).

- LLPs are formed with the objective of generating profit by two or more persons under the LLPA.

The process for creating legal persons and the processes for obtaining and recording basic and BO information are also set out in the CA and LLPA, as supplemented by specific rules (e.g., Companies (Incorporation) Rules, 2014 (CA Rules) and Limited Liability Partnership Rules, 2009 (LLP Rules); Significant Beneficial Owners Rules, 2018; Notification No. G.S.R. 110(E) dated 11 February 2022[173]). This information is publicly available at the MCA website (https://mca.gov.in).

Companies and LLPs are formed by the completion of registration requirements (CA, ss.3 and 4; LLPA, s. 12).

HUF are dealt with in Recommendation 25.

***Criterion 24.2 –*** The 2022 NRA analysed the vulnerabilities related to the availability and access to beneficial ownership information. Subsequently, India undertook a specific risk assessment of legal persons and legal arrangements in March 2023. This comprised of an assessment of the ML/TF associated with all types of legal persons that can be created in India, including private companies, public/listed companies and LLPs. This assessment included an analysis of the main vulnerabilities posed by the different types of legal entities, including typologies, as well as mitigation steps taken, with a conclusion on residual ML/TF risk posed by each entity type. This work was co-ordinated by the Department of Revenue in consultation with LEAs and agencies including the ED, MCA and FIU-IND.

***Criterion 24.3*** –

Companies

To incorporate a company, subscribers must submit a list of documents to the Registrar, including the proposed name of company, name of its directors, the memorandum which contain information on legal form and status, and the articles which contain regulations for the management of company (CA, ss.7(1). 4 and 5). Based on fulfilment of the requirements, the Registrar issues a certificate of incorporation after which legal status is obtained (CA, s.7(2) and s.9). Companies are also required to provide the Registrar with (i) verification of its registered office within 30 days of its incorporation (CA, s.12(1)); and (ii) notify the Registrar of the appointment of a director within 30 days of the appointment (CA, s.152(5)). Only individuals can be directors (s.159(1)). They are required to obtain a Director Identification Number (DIN) (s. 152(4)) which requires details such as photograph, proof of identify and proof of residence to be submitted (s.153 and Rule 9 of Companies (Appointment and Qualifications of Directors) Rules, 2014).

LLPs

To incorporate an LLP, partners must submit to the Registrar, *inter alia*, the proposed name of the LLP, name of its partners, address of its registered office, articles which contain regulations

[173] Section 67 of the LLPA empowers the Central Government to notify that certain provisions of the CA apply, and with specified modifications to LLPs. Using these powers, the Government, vide Notification No. G.S.R. 110(E) dated 11 February 2022, has notified that section 90 of the CA (Significant Beneficial Owners register), among other provisions, also apply to LLPs.

for the LLP management (LLPA, s.11 and 12). If all requirements are fulfilled, the Registrar issues a certificate of incorporation granting legal status (s.12(b)). LLPs are also required to submit the name and address of every individual who has given his/her consent to act as designated partner[174] within 30 days of his/her appointment (s.7(4)). Every LLP shall have at least two designated partners (s.7(1)).

India has a single registry of all Companies and LLPs incorporated in the country which is publicly available on MCA21 Portal (mca.gov.in).

***Criterion 24.4 –***

A company is required to maintain at its registered office copies of all documents and information as originally filed with the Registrar until its dissolution (CA, s.7(1)(4)). Companies are also required to maintain a register of members or shareholders (s.88) at their registered office of the company or at any other place in India (s.94). A company may keep in any other country a part of the register of members called "foreign register," which contains the names and particulars of the members residing outside India (s.88(4)). In such a case, the company is required to (i) transmit to its registered office in India a copy of all entries in any foreign register within 15 days after the entry is made; and (ii) keep a duplicate register of every foreign register at its registered office in India (Companies (Management and Administration) Rules, 2014, Rule 7(8)).

Companies may issue equity shares with differential rights and the register of members maintained under s.88 must contain all the relevant details of the shares along with name and address of shareholders (Companies (Share Capital and Debentures) Rules, 2014, Rule 4(6); Companies (Management and Administration) Rules, 2014, Rule 3(1); Form MGT-1).

LLPs are required to file the partnership agreement with the Registrar within 30 days of incorporation (Rule 21 of LLP Rules). LLPs are also required to notify the Registrar of any change in the registered documents as well as changes in partners within 30 days of a change (LLPA, s.25(2); Rule 21 of LLP Rules). There is no requirement for LLPs to maintain a register of partners or other information; however, this information as well as beneficial ownership information is required to be submitted to the Registrar (LLPA.s.36).

***Criterion 24.5 –*** Companies are required to submit changes to information filed with the Registrar related to c.24.3, including changes of name (CA s.4(4)), legal form (s.18), articles (s.14), address of registered office (s.12(4)), and directors (a.170(2)). New directors must obtain a DIN, which requires them to provide identification documents (see c.24.3 above). The intentional provision of false statements or the intentional omission of any material facts is an offence under the CA (ss.447-448; see c.24.13 below).

Companies are also required to maintain a register of shareholders/members, including their name, date of becoming a member and date of cessation of membership (CA, s.88(1), Form no. MGT-1). Moreover, for every new allotment of shares, a return of allotment is required to be filed with the registry within 15 days (CA, s.42(8), Form no. PAS 3). In cases of a transfer of shares, an instrument of transfer specifying the name, address and occupation of the transferee must be submitted to the company within a period of 60 days (CA, s.56(1), Form no. SH-4).

LLPs are similarly required to file changes to the Registrar, including a change in the LLP name (LLPA, s.17), partnership agreement (s.23(2)), address of the registered office (s.13(4)), name of the partners (s.25(2)), including designated partners (s.7(4)); and change in legal form (LLPA,

[174] Pursuant to s.8 of the LLPA, a designated partner is responsible for the doing of all acts, matters and things as are required to be done by the LLP in respect of compliance of the provisions of the LLPA including filing of any document, return, statement and the like report pursuant to the provisions of this Act and as may be specified in the LLP agreement.

s.55-58; CA, s.18). The notice informing of an incoming partner must contain a statement by such partner that he/she consents to becoming a partner, signed by him/her, and authenticated in the manner as may be prescribed by the government (s.25 (3)).

Companies are also required to file an annual return with the Registrar which should include a list of members along with any changes since the end of the previous financial year (CA, s.92(d), Form no. MGT-7). LLPs are similarly required to file an annual return including details of partners, including changes to partners since the close of the previous financial year (LLPA, s.35, Form no. 11).

The Registrar is required to examine every application or e-form or document filed for approval, registration, taking on record or rectification (Rule 10, The Companies (Registration Offices and Fees) Rules, 2014). In addition, the company's authorised signatory or the professionals (accountants or company secretaries) who certify e-forms are responsible for the accuracy of their content (Rule 8). The Registrar is also empowered to request further information and explanation on any document filed with him/her under any provisions of the CA (CA, s.206), also applicable for LLPs.[175]

***Criterion 24.6 –*** India has adopted a multi-pronged approach for the availability of beneficial ownership information, as follows:

a) Companies and LLPs are required to take all necessary steps to identify natural persons who are "significant beneficial owners" (SBOs) (meaning individuals who own or control the company indirectly, as described below) (CA, s.90(4)(4A)(5)).

b) Natural persons who are SBOs of a company or LLP are also required to make a declaration to the company specifying the nature of their interest and other details, and when there are any changes to this information (CA, s.90(1)).

c) Companies and LLPs are required to maintain a register of SBOs (CA, s.90(4)(4A)(5)) They are also required to file a SBO return (and if there are changes to it) with the Registrar within 30 days from the receipt of a declaration from a SBO (CA, s.90(4)). The Registrar in turn maintains an electronic register with this information, accessible to registered users.

d) Natural and legal persons who hold shares of a company but do not hold the beneficial interest176 in such shares are required to make a declaration to the company, specifying the name and other details of the person who holds the beneficial interest in the shares (CA, s.89(1)) – see c.24.12. Similarly, persons who hold a beneficial interest in the shares of a company without being legal owners are also required to provide a declaration to the company disclosing their interest (CA, s.89(2)). The company, in turn, is required to file a return informing of such declarations to the MCA Register (CA, s.89(6).

e) FIs and certain DNFBPs (i.e., TCSPs and accountants) that provide services to a company or LLP are required to perform CDD and identify the beneficial owner, and take steps to verify the identity of beneficial owner (Rule 9(1) of PML Rules). There are no legal requirements for companies and LLPs to have

[175] Notification No. G.S.R. 110(E) dated 11 February 2022.

[176] Beneficial interest in a share is defined to include, directly or indirectly, through any contract, arrangement or otherwise, the right or entitlement of a person alone or together with any other person to: (i) exercise or cause to be exercised any or all of the rights attached to such share; or (ii) receive or participate in any dividend or other distribution in respect of such share (CA, s.89(10)).

an on-going relationship with a FI or DNFBP in India, so beneficial ownership information will be available to when a company or LLP is a customer of a FI or DNFBP captured under the PMLA. More details on the definition of beneficial owner and application of obligations under the PMLA are provided under c.10.10 and R.22.

A SBO is defined as every individual, who acting alone or together, or through one or more persons or a trust, possesses one or more of the following rights or entitlements in a company, namely (CA, s.90(1); Companies (Significant Beneficial Owners) Rules, 2018, as amended, Rule2(1)(h))[177] :

a) holds indirectly, or together with any direct holdings, more than 10% of the shares;

b) holds indirectly, or together with any direct holdings, more than 10% of the voting rights in the shares.

c) has a right to receive or participate in more than 10% of the total distributable dividend, or any other distribution, in a financial year through indirect holdings alone, or together with any direct holdings.

d) has a right to exercise, or actually exercises, significant influence or control, in any manner *other than through direct holdings alone.*

If an individual does not hold any right or entitlement *indirectly* as described above, he or she is not considered to be a SBO (Explanation II to Rule2(1)(h)). An individual is considered to hold a right or entitlement "directly" in a company, if: (i) the shares in the reporting company representing such right or entitlement are held in the name of the individual; (ii) the individual holds or acquires a beneficial interest in the share of the reporting company, and has made a declaration in this regard to the reporting company (under s.89(2) of the CA).

In relation to LLPs, the same definition in the CA would apply, with slight modifications given the different structure of LLPs.[178]

The SBO reporting requirements are not applicable when the shares of a company or LLP are held by (Rule 8, SBO Rules): a holding company, provided that the holding company files SBO information (SBO information is therefore available through the holding company filings); the Central Government, a State Government or any local Authority; when a company or LLP is controlled by the Central Government or by any State Government, or partly by the Central Government and partly by one or more State Governments (SBO obligations remain for the shares controlled by other parties).

Exemptions also apply to Exchange Board of India registered investment vehicles such as mutual funds, alternative investment funds, real estate investment trusts; infrastructure investment

[177] "Control" is defined as including 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 (s.2(27)).

[178] The definition would refer to every individual, who acting alone or together, or through one or more persons or trust, including a trust and persons resident outside India, holds beneficial interests, of not less than 25% or such other percentage as may be prescribed, in contribution of a LLP or the right to exercise, or the actual exercising of significant influence or control as defined in clause (*27*) of section 2 of the CA, over the LLP (Notification No. G.S.R. 110(E) dated 11.02.2022).

trusts regulated by SEBI; investment vehicles regulated by the RBI and IRDAI (Rule 8, SBO Rules). CDD requirements described under R.10 would apply.

***Criterion 24.7 –*** A company is required to give notice to file a SBO declaration to any natural person (whether or not a member of the company) whom the company knows or has reasonable cause to believe— to:

a) be a SBO of the company or have knowledge of the identity of a SBO or another person likely to have such knowledge;

b) have been a SBO of the company at any time during the three years immediately preceding the date on which the notice is issued (s.90(5)).

A company is also required to give notice to members who hold 10% or more of its shares or voting rights or right to receive or participate in dividend (Rule 2A(2), SBO Rules).

Any individual who is a SBO is required to file a declaration to the reporting company, within thirty days of acquiring significant beneficial ownership or any change therein (Rule 3(2), SBO Rules). The company is in turn required to file a return to the Registrar with the SBO information received (Rule 4). These provisions, therefore, amount to a requirement to maintain SBO information up to date. For changes in relation to beneficial owners that are not SBOs (i.e., individuals that may own and control a company directly), the requirements under c.24.5 would ensure that information is kept up to date.

Where that person fails to give the company the SBO information required within the time specified or where the information given is not satisfactory, the company is required to apply to the Tribunal within 15 days from the expiry of the period specified in the notice (CA, s.90(6)). Such application would be for an order directing that the shares in question be subject to transfer restrictions or suspension of rights (CA, s.90(6)).

In addition, there are other provisions to compel the production of accurate information (see c.24.5 and c.24.13):

- the company's authorised signatory or the professionals who certify e-forms are responsible for the correctness of their content as well as of the enclosures (Rule 8, The Companies (Registration Offices and Fees) Rules, 2014);
- the Registrar is required to examine an application or e-form or document for approval, registration, or rectification (Rule 10);
- the Registrar is also empowered to call for further information and explanation on any document filed with him/her under any provisions of the CA (CA, s.206) and those powers also apply in relation to LLPs.[179]

***Criterion 24.8 –*** The CA places responsibilities on the company's officers[180] to provide information to the Registrar or produce documents upon an inspection (CA, ss.206-207). These provisions are sufficiently broad to cover all basic information and available BO information. As noted in c.24.6 and 24.3, there are requirements for companies, through their authorised signatories, accountants or company secretaries, to file basic and beneficial ownership information. Also, any officer of the company who is in default with these obligations can be sanctioned (see c.24.13 below).

[179] Notification No. G.S.R. 110(E) dated 11 February 2022.

[180] Officers include any director, manager or key managerial personnel or any person in accordance with whose directions or instructions the Board of Directors or any one or more of the Directors is or are accustomed to act (CA, s.2(59)).

***Criterion 24.9 –*** The Registrar maintains information and records of companies and LLPs, including most basic (except a register of shareholders) and BO information, even after their dissolution of a company or LLP. The CA requires electronic filing of records with the registry which also maintains the records in the electronic form. There are no provisions which allow the registry to remove any record and therefore records are kept indefinitely (see also The Disposal of Records (in the Offices of the Registrars of Companies) Rules, 2003, which requires the register of companies as well as information in relation to any company in operation to be preserved permanently (Rule 3).[181] LLP records must be maintained for a minimum period of 5 to 21 years depending on the type of record and records submitted electronically are preserved permanently.

When the affairs of a company have been completely wound up and it is about to be dissolved, the books and papers of such company and those of the company liquidator may be disposed of in such manner as the court directs (CA, s.347(1)). As such, it is not ensured that records will be kept for at least five years after dissolution. This potential gap would mainly relate to the maintenance of the share register as well as full BO information maintained by the company after dissolution. Most other basic information as well as SBO information is required to be kept by the Registrar as well. The CA also provides that, after the expiry of five years from the dissolution of the company, no responsibility shall devolve on the company, the company liquidator, or any person to whom the custody of the books and papers has been entrusted (CA, s.347(2)). Similar rules are provided for LLPs, except that their books and papers can be disposed of as per the direction of a quorum of three quarters of partners in case of voluntary winding-up (Rule 55, The Limited Liability Partnership (Winding-up and Dissolution) Rules, 2012). Basic and SBO information of LLPs is nonetheless required to be kept by the Registrar.

In respect of companies under liquidation for their inability to pay debts under the Insolvency and Bankruptcy Code, 2016, the books and records of such Companies shall be preserved by the liquidator for a period of 8 years after the dissolution of the Company, (Regulation 41, the Insolvency and Bankruptcy Board of India (Voluntary Liquidation Process) Regulations, 2017).

REs are required to maintain records of documents evidencing identity of clients and beneficial owners, as well as account files and business correspondence relating to clients (PMLA, s.12(1)). Records must be kept for a period of five years after the business relationship between a client and the RE has ended or the account has been closed, whichever is later (PMLA, s.12(4) and s.12(1)(e)).

***Criterion 24.10 –*** Basic and beneficial information is publicly available on-line, via the MCA website, ensuring timely access for competent authorities. LEAs also have powers in their respective statutes to require persons to provide information and penal provisions in case of default. Powers of LEAs to obtain information has been specified in response to Recommendation 31. Moreover, the Registrar is empowered to call for further information and explanation on documents and information filed by a company or LLP (CA, s.206).[182]

***Criterion 24.11 –*** There are no references to bearer shares or bearer share warrants in the Companies Act, 2013. Company law requires that every company maintain a register of members or shareholders, indicating the identification details (name, address, identification document) number of shares maintained by each member and the share's distinctive number

[181] Before the Companies Act, 2013., company records were not required to be electronically filed and Disposal of Records (in the Offices of the Registrars of Companies) Rules, 2003 required returns and other registered documents to be kept for a minimum term of five years, whereas the registry of companies and certain registered documents of companies in operation were required to be preserved permanently.

[182] Extended to LLPs as per Notification No. G.S.R. 110(E) dated 11th February 2022.

(CA, s.88(1)); Rule 3(1) the Companies (Management and Administration) Rules, 2014; Form MGT-1). Companies making public offers are required to issue the securities only in dematerialised form by complying with the provisions of the Depositories Act, 1996 (CA, s.29(1)(a)).

In addition, as referenced in c.24.6, individuals holding beneficial interests, of not less than 25% in shares are required to make a declaration to the company, specifying the nature of their interest, Companies are required to maintain a register of the interest declared by individuals as described above, including their names, date of birth, address, details of ownership in the company and such other details as may be prescribed (CA, s.90(1) and (2)).

***Criterion 24.12 –*** The CA does not contain specific provisions on nominee ownership; however, the situation that nominal and beneficial ownership can exist separately is acknowledged in section 89(1) of the CA. That section casts an obligation on a person who holds shares of a company but does not hold beneficial interest[183] in such shares, to make a declaration to the company specifying the name and other details of the person who holds the beneficial interest in such shares. In addition, persons who hold a beneficial interest in the shares of a company without being legal owners are also required to provide a declaration to the company disclosing such interest (CA, s.89(2)). The company, in turn, is required to file a return informing of such declarations to the MCA Register (CA, s.89(6)). Moreover, persons acting as a nominee shareholder for another person, by way of business, are AML/CFT REs (PMLA, s.2(1)(sa)(vi), Notification S.O.2135(E) of 9 May 2023). They are subject to CDD obligations and required to identify the customer and the customer's beneficial owner and verify their identity (see c.22.1 and c.10.11).

Further, India law provides for a specific prohibition of "benami" transactions, outside a fiduciary relationship (see c.24.7 above). An arrangement where (a) a property is transferred to, or is held by, a person, and the consideration for such property has been provided, or paid by, another person; and (b) the property is held for the immediate or future benefit, direct or indirect, of the person who has provided the consideration, is considered to be a "benami transaction" and prohibited in India (The Prohibition of Benami Property Transactions Act, ss.2 and 3).

Nominee directors are permissible in India. A nominee director is defined as a director nominated by any financial institution, or of any agreement, or appointed by any Government, or any other person to represent its interests (CA, s.149(7)). The circumstances for their appointment are also provided in the CA: a company's board may appoint any person as a director nominated by any institution based on the law or of any agreement or by the Central or State Government by virtue of its shareholding in a Government company (s.161(3)). Companies are required to file with the Registrar form DIR-12 containing the name of nominator, within thirty days from the appointment of every nominee director and key managerial personnel (CA, s.170(2)). Designated partners of LLPs would be subject to the SBO disclosure rules that would require them to disclose whether they act on behalf of another person.

***Criterion 24.13 –*** Sanctions are available for natural and legal persons that fail to comply with the requirements in R.24. Overall, they appear to be proportionate and dissuasive, although monetary sanctions may not be sufficiently dissuasive for larger businesses. They are:

[183] Beneficial interest in a share is defined to include, directly or indirectly, through any contract, arrangement or otherwise, the right or entitlement of a person alone or together with any other person to: (i) exercise or cause to be exercised any or all of the rights attached to such share; or (ii) receive or participate in any dividend or other distribution in respect of such share (CA, s.89(10)).

*Basic Information*

a) ***Companies*** If a company does not maintain a register of members or fails to maintain it in accordance with the provisions of the CA, the company is liable to a penalty of INR 300 000 (EUR 3 304) and every officer of the company who is in default shall be liable to a penalty of INR 50 000 (EUR 551) (CA, s. 88(5)). Any designated personnel, such the managing director, full-time director in charge of finance, CFO, or others assigned by the Board to ensure compliance with requirements to maintain company records fail to do so, they could be subject to a fine of at least INR 50 000 (EUR 551), extendable to INR 500 000 (EUR 5 507) (CA, s.128(6)). Also, if the companies and officers fail to maintain a register of directors and key managerial personnel and file it with Registrar, they may be subject to a fine of INR 50 000 (EUR 550) (CA, s.172 read with s.170). In the case of continuing default, companies could be subject to a fine of INR 500 (EUR 5) per day up to INR 300 000 (EUR 3 304) and the officer in default could be subject to a fine of INR 100 000 (EUR 1 101) (CA, s.172 read with s.170). The Registrar can deregister companies when they have failed to commence business within one year of incorporation; when they are not carrying out business or operations for a period of two immediately preceding financial years and have not made an application for dormant status; and when it ascertains that the company is not carrying out business or operations by visiting its address (CA. s.248).

b) ***LLPs:*** If an individual provides a statement under the incorporation form that they either know to be false or do not believe to be true, they could face imprisonment for up to two years and a fine ranging from INR 10 000 (EUR 110) to INR 500 000 (EUR 5 506) (LLPA, s.11(1)(c) and (3)). Any person that provides a false statement in any return, statement or other document required under the LLPA could be subject to imprisonment up to 2 years along with a fine ranging from INR 100 000 (EUR 1 100) to INR 500 000 (EUR 5 506) (LLPA, s.37). An LLP that fails to maintain the books of account and other records and audit could be subject to a fine ranging from INR 25 000 (EUR 275) to INR 500 000 (EUR 5502) and designated partners could be subject to a fine ranging from INR 10 000 (EUR 110) to INR 100 000 (EUR 1 100) (LLPA, s. 34(6)). Similar to companies, the Registrar also has powers to deregister an LLP deemed inactive (LLP Rules, 2009; Rule 37).

*Beneficial Ownership Information and other requirements*

a) ***Companies-*** A person that fails to make a declaration in respect of his/her beneficial interest (i.e., nominator) in a share, may be subject to a fine of INR 50 000 (EUR 550), and in case of continuing default, to a further penalty of INR 200 per day with maximum of INR 500 000 (EUR 5 506) (CA, s.89(5)). The same fines apply to a nominee who fails to disclose that shares are held on behalf of a nominator and identify such a nominator (CA, s.89(5)). A company that fails to file a return identifying nominee shareholders and nominators as well as every officer of the company who is in default are punishable with a daily penalty of INR 1 000 up to a maximum penalty of INR 500 000 (EUR 5 506), in the case of a company and INR 200 000 (EUR 2 202) and in case of an officer who is in default (CA, s.89(5)(7)). Moreover, the holder of beneficial interest (nominator) or any person on his/her behalf cannot enforce any right in relation to the shares in case of failure to make a declaration (CA, s.89(8)).

b) If a company fails to maintain a SBO register and file it with the Registrar, or take necessary steps to identify an individual who is an SBO, for a penalty ranging from INR 100 000 (EUR 1 101) to INR 1 million (EUR 11 013) may be applied (CA, s.90(11)), and in case of continuing failure, the fine may extend to INR 1 000 (EUR 11) per day. A person who fails to declare that he/she is an SBO, is subject to the same penalty (CA, s.90(10)(11)). A company and any officer that fails to provide information or documents to the Registrar may be subject to a fine up to INR 100 000 (EUR 1 101), and, in case of continue failure, to an additional fine up to INR 500 per day (EUR 5) (CA, s.206 (7)). Any person that fails to maintain records after the winding up of a company as required (see c.24.9), is punishable with a fine of up to INR 50 000 (EUR 550) (CA, s.347 (4)).

c) ***LLPs***: Similar to companies, LLPs that fail maintain SBO register and file it with Registrar, or to take necessary steps to identify an individual who is a SBO, it is liable for penalty ranging from INR 100 000 (EUR 1 101) to INR 1 million (EUR 11 013) and in case of continuing failure, the fine may extend to INR 1 000 (EUR 11) per day (LLPA, s. 67; CA, s.90(11)). LLPs that fail to maintain books of accounts, or prepare a statement of solvency and audit when required, are punishable with a fine ranging from INR 25 000 (EUR 275) to INR 500 000 (EUR 5502) and designated partners are punishable with a fine ranging from INR 10 000 (EUR 110) to INR 100 000 (EUR 1 100) (LLPA, s.34(5)).

***Criterion 24.14 –***

a) Basic information in the company registry is publicly accessible online, including for foreign competent authorities. It does require foreign competent authorities to register to obtain access and purchase the required documentation.

b) Competent authorities have powers under their respective statutes to exchange information on shareholders to foreign counterparts who make such requests as part of assistance in ML investigations (PMLA, s.58).

c) Beneficial ownership information is available at the BO register. As indicated above, this data is available for registered users. Competent authorities' investigative powers can also be used, in accordance with domestic law, to obtain BO information on behalf of foreign counterparts (PMLA, ss.56 and 58).

***Criterion 24.15 –*** India monitors the quality of assistance it receives in response to requests for basic and BO information or for locating beneficial owners abroad. For instance, the ED has a dedicated unit, the Overseas Investigation Unit, responsible for coordinating and monitoring the international cooperation, both formally and informally. This unit analyses the quality of assistance received and is also responsible for providing feedback to foreign counterparts. India indicated that each LEA has a mechanism to monitor the quality of assistance; but no information was provided to demonstrate this. Recently, the Central Authority of India introduced a portal for digital management of cases of outgoing MLA requests to streamline the process.

## *Weighting and Conclusion*

India has implemented mechanisms to ensure the availability of basic information for legal persons with the MCA Registry, and BO information through the MCA Registry, companies, or from FIs or DNFBPs in the AML/CFT framework. There remain some minor shortcomings. In particular, monetary sanctions may not be sufficiently dissuasive for larger businesses (c.24.13)

and it is unclear if the quality of basic and BO information received by India is sufficiently monitored (c.24.15). These gaps carry less weight considering the overall comprehensive legal framework in place with respect to other requirements.

**Recommendation 24 is rated largely compliant.**

## Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its last MER, India was rated partially compliant with the former R.34. Deficiencies included the absence of a requirement to obtain, verify and retain adequate, accurate and current information on the beneficial ownership and control of private trusts; and lack of measures that guarantee that minimal adequate and accurate information concerning the beneficial owners of private trusts could be obtained or accessed by the competent authorities in a timely fashion.

There are four categories of express trust or similar legal arrangements in India which fall within the FATF's definition.

1. Private trusts: to benefit selected persons;
2. Charitable or public trusts (including wakfs): to benefit the public at large;
3. Societies registered under Societies Registration Act, 1860;
4. Hindu Undivided Family Businesses (HUFs)[184].

***Criterion 25.1 –***

a) Persons acting as (or arranging for another person to act as) a trustee of an express trust on a professional basis are REs under the PMLA (PMLA, s.2(1)(sa)(vi) combined with Notification S.O. 2135(E) of 9 May 2023). Professional trustees are subject to CDD and record-keeping obligations on their clients (i.e., the settlor and beneficiary) (see c.22.1 and c.10.11).

Beneficial owner is defined in the PMLA as an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and *includes* a person who exercises ultimate effective control over a 'juridical' person (PMLA, s.2(1)(fa)). It is not clear if the definition includes a natural person who exercises ultimate effective control over a legal arrangement; however, the PML Rules clarify how the beneficial owner of trusts and other legal arrangements should be identified (see below).

Where the client is a trust, professional trustees are required to identify the settlor, the trustee(s), the beneficiaries with 10% or more interest in the trust as well as any other natural person exercising ultimate effective control over the trust through a chain of control or ownership (PML Rule 9(3)(e)). In addition, professional trustees are also required to collect information on the names of the beneficiaries, trustees, protector (if any) and settlor of the trust (PML Rule 9(8)(v)).

Professional trustees are required to apply CDD measures to existing clients on the basis of materiality and risk and conduct due diligence on such existing relationships at appropriate times or as may be specified by the regulator, taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained (PML Rule 9(12)(iii)). Clients are required to share with REs including professional trustees any updates related to CDD data within 30 days of the change (PML Rule 9((B)).

[184] See section 1.4.5 in Chapter 1.

Professional trustees are also required to verify the identity of the client and take all steps to verify the identity of the beneficial owner (PML Rule 9(1)(c)). A list of sources and documents which are acceptable for verification of identity, which represents reliable, independent sources of identification data. is provided (PML Rule 9 (4), (6-10)). Those requirements would support the availability of adequate, accurate and current information.

There is no general requirement for trustees that are not acting in the course of business to obtain and hold all information covered by this sub-criterion. Nonetheless, some records are required to be available on the basis of other requirements which apply to the different types of trusts that can be created in India, as described below. However, they do not fully amount to a requirement for trustees to hold adequate, accurate and current information on all the parties to the trust and other natural persons exercising ultimate effective control over the trust.

Private Trusts

Private trusts having taxable income over INR 250 000 (EUR 2 727) must apply for a Permanent Account Number (PAN) and provide a copy of the trust deed (Income Tax Act, 1961, s.139A, Form 49A). The trust deed may have details of the settlor, beneficiary, trustee(s) and protector. In addition, trustees of business trusts with the minimum income referenced above are required to submit annual income tax returns in respect of the trust, including particulars of settlors, trustees and beneficiaries (Income Tax Act, ss. 139 and 160; form ITR-5).

Charitable/Public Trusts

States can enact their own legislations for incorporation and regulations of public trusts – *e.g.,* Bombay Public Trust Act, 1950, applicable in the State of Maharashtra, The Madhya Pradesh Public Trusts Act, 1951 and The Rajasthan Public Trust Act, 1959. For instance, in relation to the Bombay Public Trusts, trustees are required to make an application to Charity Commissioner for the registration of the public trust (s.18) and such an application requires the name and addresses of trustees and manager; changes to registration must be reported (s.22). In addition, the accounts of Bombay public trusts must be audited and the auditor is required to submit details names and PAN of the trust and of all trustees (Rule 19(2A) of the Maharashtra (Bombay) Public Trust Rules, Schedule IX-D). The Charity Commissioner has powers to request trustees of public trusts to produce any documents or book of accounts in the possession or under the control of the trustee or any person connected with the trust (s.37, Bombay Public Trust Act).

Wakfs are required to be registered with the State Boards (Waqf Act, ss.36-37). The register maintained by the Boards are required to include copies of the waqf deed when available and the class of the waqf, the name of the *mutawallis* (i.e., administrator/ trustee). The Board is also required to maintain a record containing the details regarding the beneficiaries of every waqf (Waqf Act, s.32(2)).

Trustees are also required to submit an annual return of income for charitable trusts, disclosing details of trustees, settlors and beneficiaries (Income Tax Act, s.139(4A), Form ITR-7).

Societies

To register a society, it is required a memorandum of association containing the names, addresses and occupations of the governors, council, directors, committee or other governing body to whom, by the rules of the society, the management of its affairs is entrusted (Society Registration Act, 1860, ss.1 and 2). This information must also be filed on annual basis (s.4).

HUFs

The *karta* (administrator of the trust, generally the most senior member of a family) has fiduciary duties towards other members of the HUF[185]. Moreover, the karta is required to file Income Tax Form 49A (application for allotment of PAN) stating his or her details and name and address of all the coparceners (family members) and submit a document to proof his or her identity.

b) Professional trustees are required to hold account files and business correspondence relating to their clients (PMLA, s.12). They are also required to obtain information on (other) trustees (PML Rule 9(8)(v)). In addition, other requirements, described below, are also provided for the different types of trusts. These requirements may support the availability of some basic information on regulated agents of and service providers to the trust. However, they do not amount to a requirement to hold basic information on other regulated agents and service providers to the trust.

*Private trusts* –Trustees of private trusts are required to keep clear and accurate accounts of the trust property (Indian Trust Act, s.19). Beneficiaries have the right to inspect and take copies of accounts of the trust property and the vouchers (if any) by which they are supported, the cases submitted and opinions taken by the trustee for his/her guidance in the discharge of his/her duty (s.57). India considers that, as service providers to the trust would charge money for the services they provided, basic information on such service providers would form the part of the books and vouchers required to be kept.

*Charitable/Public trusts* – Requirements under the Income Tax Act concerning tax exemptions would require trustees of public trusts to maintain books of accounts, audited by a chartered accountant, and produce an audit report at the time of filing of a return of income. In relation to Bombay Public Trusts, the trustee is required to make available to the auditor all books, vouchers, other documents and records in the possession of or under the control of the trustee (Bombay Public Trust Act, s.33). India considers that, as service providers to the trust would charge money for their services, basic information on such service providers would form the part of the books and vouchers required to be kept.

*Societies* – There are no specific requirements related to this sub-criterion in the Society Registration Act, 1860. India advises that state law requirements would generally cover maintenance of book of accounts and preparation of financial statements (e.g., Haryana Registration and Regulation of Societies Act, 2012. Similar to what is stated above, a service provider to the trust would charge money for the services provided, and therefore such transaction would form the part of the books and vouchers which would contain the basic information of the service provider.

*HUFs* – There is no specific requirement for a HUF to hold basic information on other regulated agents of, and services provides to the karta.

c) As indicated under c.25.1.a above, professional trustees are required to perform CDD and obtain and hold information on the parties of the trust. Professional trustees are also required to hold the names of other trustees and protector (if any), account files and business correspondence relating to their clients (PMLA, s.12). Whilst this may include some basic information on regulated agents of and service providers to the trust, this does not amount to a requirement to always hold basic information on all service providers to the trust.

[185] N.C.T. Chidambaram Chetiar vs Ct. A. Ct. Subramaniam And Ors, AIR 1982 Mad 228.

Professional trustees are required to keep records for a period of five years after the business relationship between a client and the FI has ended (PMLA, s.12(4) and s.12(1)(e)).

***Criterion 25.2 –*** For trusts having a professional trustee or a relationship with another RE, such REs are required to apply CDD measures to existing clients on the basis of materiality and risk and conduct CDD on such existing relationships at appropriate times or as may be specified by the regulator, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained (PML Rule 9(12)(iii)). For professional trustees, the regulator has not specified the appropriate times for CDD update. Clients are required to inform professional trustees of changes to CDD data within 30 days of the change.

Professional trustees and REs are also required to verify the identity of the client and take all steps to verify the identity of the beneficial owner (PML Rule 9(1)(b)). A list of sources and documents which are acceptable for verification of identity, which represents reliable, independent sources of identification data. is provided (PML Rule 9 (4), (6-10)). Those requirements would support the availability of adequate and accurate information.

Some information may also be held accurate and update based on other trust law and tax law requirements described in c.25.1 above, but those do not comprehensively address all the requirements of that criterion.

***Criterion 25.3 –***

REs are required to ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out occasional transactions of equal to or exceeding INR 50 000 (approx. EUR 563) (PML Rule 9(10)).

***Criterion 25.4 –***

There are no legal restrictions on trustees providing competent authorities or FIs and DNFBPs with any information relating to trusts. Professional trustees are REs under the PMLA (Notification S.O. 2135(E) of 9 May 2023).

In addition, the 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.

***Criterion 25.5 –***

Competent authorities and in particular LEAs have legal powers under respective statutes (PMLA, Income Tax Act, UAPA etc) to obtain access to any information held by any person, including trustees, FIs, and DNFBPs. This would include access on beneficial ownership and control of the trust including the beneficial ownership, residence of the trustee, and any assets held or managed by the financial institution or DNFBP in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction (PMLA, s.50). In addition, the PMLA has empowered the Director of FIU-IND to compel production of records on a timely fashion, discovery and inspection and call for examination of witnesses and documents (s.50).

***Criterion 25.6 –*** The provisions for cooperation with competent authorities in other countries described under R.37 and R.40 also apply to the exchange of information on trusts and legal arrangements.

a) Basic information of public trusts and societies may be accessed by domestic authorities and shared with foreign counterparts (PMLA, ss.58 and 56).

b) Upon request, Indian competent authorities can provide information on trusts and other legal arrangements (PMLA, ss.58 and 56). This would include CDD collected by professional TCSPs and other REs.

c) The competent authorities can use all its domestic investigative powers to conduct investigation on behalf of foreign counterparts also (PMLA, s.58).

***Criterion 25.7 –*** In India, the trustees have fiduciary duties and are legally liable for any failure to perform the duties relevant to meeting their obligations.

Professional trustees are REs under the PMLA and subject to monetary sanctions if they fail to observe the record-keeping requirements (PMLA, s.13(2), s.12) or to provide the Direct FIU-IND with access to information (PMLA, s12A) (see also R.35). Monetary sanctions range from INR 10 000 (EUR 111) to INR 100 000 (EUR 1113) for each failure. These sanctions are proportionate as they would directly correlate to the number of instances of violations identified and may be calibrated depending on the gravity of the offenses. However, these sanctions may not always be dissuasive, in particular for larger institutions, but other sanctions provided in the context of the Indian Penal Code for fraudulent cases may have a dissuasive effect (see below).

In respect of charitable/public trusts, sanctions would be provided in the respective state statutes. For instance, Bombay Public Trusts Act, 1950 (ss.66-67) specify sanctions for failure to apply for registration or to notify changes (which are subject to a fine of INR 10 000 (EUR 113)); however, those sanctions are not dissuasive. That Act also provides for suspension, removal and dismissal of trustees if they make persistent default in the submission of accounts report or return (s.41.D).

For serious breach of trustee duties, trustee can be liable for imprisonment, or a fine or both. Indian Penal Code (IPC), s.405). This would apply to any person entrusted with property who dishonestly misappropriates or converts or uses or disposes the property in violation of any direction of law or of any legal contract, express or implied, and commits "criminal breach of trust" (s.405). The punishment for criminal breach of trust may be extended up to a period of 3 years of imprisonment or fine or both (s.406). In addition, “cheating by personation”[186] is an offense which is punishable with imprisonment that may extend to 3 years or fine or both, and this may be relevant in the context of c.25.3 (IPC, s.416). The amount of the fine is determined by the judicial authorities taking into account various parameters including the gravity of offence.

**Criterion 25.8 –** Indian law enforcement authorities have legal powers under respective statutes to obtain timely access to information held by any person, including trustees (see R.31).

Provisions of the Indian Penal Code provide for imprisonment, fine or both in cases of failure to grant public authorities timely access to information (see table below).[187] However, there is lack of proportionality due to a narrow range of sanctions, as either a low fine or an imprisonment sanction (or both) apply.

[186] This refers to cheating by pretending to be some other person, or by knowingly substituting one person for or another, or representing that he or any other person is a person other than him or her or such other person really is.

[187] In December 2023 (after the ME on-site visit), the IPC has been replaced by Bhartiya Nyay Sanhita, 2023. The maximum fines related to the relevant infractions (now sections 204 to 208) have been to INR 10 000 (EUR 111).

| Provision under India Penal Code | Punishment |
|---|---|
| 172. Absconding to avoid service of summons or other proceedings | Simple imprisonment for a term which may extend to one month or fine which may extend to INR 1 000 (EUR 11), or both. |
| 174. Non-attendance in obedience to an order from public servant | Simple imprisonment for a term which may extend to one month or fine which may extend to INR 1 000, or both |
| 175. Omission to produce document to public servant by person legally bound to produce it | Simple imprisonment for a term which may extend to one month or fine which may extend to INR 1 000, or both |
| 176. Omission to give notice or information to public servant by person legally bound to give it. | Simple imprisonment for a term which may extend to one month or fine which may extend to INR 1 000, or both |
| 177. Furnishing false information | Simple imprisonment for a term which may extend to six months, or fine which may extend to INR 1 000, or both |
| 178. Refusing oath or affirmation when duly required by public servant to make it. | Simple imprisonment for a term which may extend to six months, or fine which may extend to INR 1 000, or both |
| 181. False statement on oath or affirmation to public servant or person authorised to administer an oath or affirmation | imprisonment for a term which may extend to three years and a fine (to be defined by the judicial authority) |

Failure to furnish an Income Tax return is subject to a fee of INR 5 000 (EUR 56) depending on the type of return (Income Tax Act, s. 271F) plus an assessment of the income due. These sanctions may not be dissuasive in all cases.

### *Weighting and Conclusion*

India has some minor shortcomings in its framework relating to the transparency and BO Information of legal arrangements. In particular, the requirements are more limited in respect to trusts administered by non-professional trustees, access to adequate, accurate and current information on the identity of the settlor, the trustees, the protector and the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust may not always be ensured (c.25.1 and c.25.2). Sanctions to ensure access to information are not always proportionate (c.25.8).

**Recommendation 25 is rated largely compliant.**

## Recommendation 26 – Regulation and supervision of financial institutions

In its last MER, India was rated partially compliant with former R.23, because (i) the PMLA did not apply to commodities futures brokers; (ii) fit and proper testing by regulators prior to appointment did not apply to non-executive Directors; (iii) Authorised Persons and Payment Service Providers, including India Post, had only recently been brought under the PMLA, and hence it was too early to assess effectiveness; (iv) there were no inspections or ongoing monitoring by the Ministry of Finance of India Post; (v) there were concerns that the regulators' procedures for targeting on-site inspections do not adequately take into account the AML/CFT risks of individual institutions. Its 8th FUR concluded that most deficiencies were at least largely

addressed and that India's level of compliance with former R.23 was essentially equivalent to largely compliant.

**Criterion 26.1 –**

A "Regulator" is defined in the PML Rules as a person or an authority or a government which is vested with the power to license, authorise, register, regulate or supervise the activity of FIs, as notified by the Indian government (Rule 2(fa)). The regulator can also be the Director of the FIU if so notified (Rule 2(fa)). Regulators have the power to issue guidelines incorporating the preventive measures requirements (PML Rule 9(14)). Regulator's powers include thus powers to regulate and supervise FIs' compliance with AML/CFT requirements. General powers to supervise, regulate and issue necessary directions are vested in the respective regulator under each of the parent legislation, as summarised below:

| Financial Institutions covered | Regulator/ Supervisor empowered | Parent Legislation | Specific Section / Rule reference |
|---|---|---|---|
| **Banking Companies** | RBI | Banking Regulation Act, 1949 (BR Act) | Sections 22, 35A and 56 |
| **Rural Co-operative Banks** | RBI/ NABARD[188] | BR Act | Sections 22, 35A and 56 |
| **Regional Rural Banks** | RBI/ NABARD[189] | Regional Rural Banks Act, 1976 | |
| **Non-Banking Financial Companies** | RBI | RBI Act | Sections 45-IA, 45L |
| **Payment Systems Operator** | RBI | PSS Act | Sections 3, 10 and 17 to 19. |
| **Authorised persons for foreign exchange[190] and MTSS Agents** | RBI | FEMA | Sections 10 to 12 |
| **Housing Finance Companies** | RBI/ National Housing Bank (NHB) | NHB Act | Section 29A |
| **Financial market intermediaries** | SEBI | SEBI Act | Sections 11(2) and 11B |
| **Insurance companies and intermediaries** | IRDAI | Insurance Act<br>IRDA Act | Section 34<br>Section 14 |
| **Pension Funds and intermediaries** | PFRDA | PFRDA Act | Section 15 |
| **FIs registered in the IFSC** | IFSCA | IFSCA Act | Sections 12.13 and 21 |
| **Post offices** | RBI/ Department of Post | The Government Savings Promotion Act 1873 and Government Savings Promotion General Rules 2018 | |
| **Online Payment Gateway Service Providers (OPGSP)** | RBI | PSS Act | Sections 3, 10 and 17 to 19 |

***Criterion 26.2*** **–** Banking companies are required to be licensed by the RBI (BR Act, ss.22(1), 23 and 56). Banks in the IFSC are licensed by the IFSCA, following the same requirements set in the

[188] National Bank for Agriculture and Rural Development.
[189] National Bank for Agriculture and Rural Development.
[190] This includes (i) Full-fledged Money Changers (FFMCs); (ii) Authorised Dealers Category I (Commercial Banks, State Cooperative Banks, Urban Cooperative Banks), (iii) Authorised Dealers Category-II (other types of banks including Regional Rural Banks, Small Finance Banks, Payments Banks, as well as Systemically Important Non-Deposit taking NBFC – Investment and Credit Companies); (iv) Authorised Dealer Category-III (these are selected financial institutions and other institutions who are administered by their respective sectoral regulators).

BR Act (IFSCA Act, s.13(4) and First Schedule).[191] "Banking company" are defined as a company which transacts the business of banking in India (BR Act, s.5 (c)). Although there are no specific provisions in the BR Act or elsewhere expressly 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. There is a requirement for the bank to be controlled by residents in India at all times (Guidelines for 'on tap' Licensing of Universal Banks in the Private Sector, para.2(I)(a)).

Non-banking Financial Companies (NBFCs) are required to register with the RBI (RBI Act, s. 45-IA). Payment Systems Operators, Full-fledged Money Changers, Authorised Dealers in foreign exchange Categories-II and III as well as MTSS Agents require RBI authorisation (PSS Act, s.4; FEMA, s.10(1)).

The Securities and Insurance sectors are not required to be licensed, as required under the standard. Financial market intermediaries require registration with the SEBI (SEBI Act, s.12). Insurance companies and intermediaries require registration with the IRDAI (Insurance Act, 1938; ss. 3 and 42D. Pension funds and intermediaries require registration with PFRDA (PFRDA Act, s.27). Non-bank FIs in the IFSC require registration or authorisation by the IFSCA (IFSCA Act, s.13(4) and First Schedule), following the same requirements established for similar FIs established in India (e.g., RBI licensing requirements would be followed for IFSC banks, IRDAI requirements for IFSC insurance companies).

Companies can apply for registration with the RBI as Housing Finance Companies (NHB Act, s.29A, Housing Finance Company Directions, 2021).

***Criterion 26.3 –***

Banks

Licensing

Promoters/ Promoter Groups should be 'fit and proper' in order to be eligible to promote Universal Banks (Guidelines for 'on tap' Licensing of Universal Banks in the Private Sector dated 1 August 2016, para. 2(B)).[192]. A promoter is defined as a person who together with his relatives, is in effective control of the bank by virtue of his ownership of voting equity shares and includes, wherever applicable, all entities which form part of the Promoter Group. A Promoter Group includes a promoter and his/ her relatives but does not include other associates. Promoters are also required to provide information on individual promoters behind the group (i.e., individuals that own or control at least 10% of shares/ voting rights). Such individuals are required to provide self-declarations, including details on criminal convictions (Annex II, Appendix I)

The RBI would assess the 'fit and proper' status of the applicants including their record of sound credentials, integrity and professional track record in the last 10 years (Guidelines for 'on tap' Licensing of Universal Banks in the Private Sector dated 1 August 2016, para. 2(B))[193]. RBI also seeks input from enforcement and investigative agencies like ITD, CBI, and the ED. Those

[191] Public Sector Banks do not require banking license from RBI to do the business of banking as they are statutory bodies. Similarly, Regional Rural Banks also do not require banking license from RBI; they are owned by Central Government, concerned State Government and the sponsor bank in the proportion of 50:15:35.

[192] Similar provisions are contained in the Guidelines for 'on tap' Licensing of Small Finance Banks in the Private Sector dated 5 December 2019, Guidelines for Licensing of New Banks in the Private Sector; or licensing guidelines for payments banks dated 27 November 2014.

[193] Similar provisions are contained in the Guidelines for 'on tap' Licensing of Small Finance Banks in the Private Sector dated 5 December 2019.

requirements may not be sufficient to prevent criminal associates from holding (or being a beneficial owner of) a significant controlling interest in a FI.

In relation to Payment Banks, the Guidelines for Licensing of Payments Banks require individual promoters to provide information on their background and experience but no information on criminal convictions. The Guidelines also note that RBI may apply additional criteria to determine the suitability of applications, in addition to the prescribed 'fit and proper' criteria (para.15(I)); however no further documentation was available specifying the criteria. and the guidelines do not include details on any checks that would be performed in this regard. No information has been provided on the process for licensing Local Area Banks (LABs). For the licensing of UCBs, the RBI relies on details available on the Registrar of Co-operative Societies, which would cover all persons that are members of the co-operative as well as promoters. There are no provisions regulating the market entry measures that the RBI would apply to UCBs. The RBI advises that it does not currently accept new applications for Payment Banks, LABs and UCBs.

Change in control

The acquisition of banks' shares resulting in change in shareholding of 5% or more of the paid-up share capital or total voting rights of a banking company is subject to prior approval by the RBI (BR Act, s. 12B). The applicant should be a fit and proper person to acquire shares or voting rights (BR Act, s. 12B(2)). Information on the applicant's beneficial owner(s) is required (Form A, Guidelines on Acquisition and Holding of Shares or Voting Rights in Banking Companies) 2023). A bank board of directors is required to put in place 'fit and proper' criteria for major shareholders, which include information on any proceedings of a serious nature or of any investigation which may lead to such proceedings (Acquisition and Holding of Shares or Voting Rights in Banking Companies Directions, 2023. s.4.3 and Annex II). RBI would undertake due diligence to assess the 'fit and proper' status of the applicant (s.4.4) and the beneficial owner. The RBI can make enquiries with revenue authorities and investigation agencies and other regulators and take into account the outcome of these enquiries when considering the application (Directions, Annex II; Guidelines on Acquisition and Holding of Shares or Voting Rights in Banking Companies, 2023; s.3).

Appointment of key managerial personnel

Prospective directors of a banking company must furnish extensive details of proceedings against the candidate including prosecution (both against self and against entities interested in/ having substantial shareholding in/being associated with) for violation of economic laws and regulations, and criminal conviction pending or commenced or resulting in conviction; details of conviction involving by a Criminal Court of an offence involving moral turpitude or otherwise, or convicted in any court of law; being subjected to any investigation/vigilance/matters of enquiry from any of the previous employers or government departments or agency (both against self and against entities interested in/ having substantial shareholding in/being associated with-); violation of rules/ regulations/ legislative requirements by customs/ excise/ income tax/ foreign exchange/ other revenue authorities, if any; and if reprimanded, censured, restricted, suspended, barred, enjoined, or otherwise sanctioned by regulators, professional organisation, government agency, or court because of professional conduct or activities, details thereof (Circular dated March 31, 2020[194], Declaration of Undertaking). Banks are expected to have their own Board approved policy/procedure laying down the criteria for recruitment, which shall include fit and proper requirements, including a declaration of undertaking by the directors, with information on criminal convictions (Circular of 24 June 2004 on Fit and proper criteria for

[194] Appointment of Managing Director and Chief Executive Officer (MD & CEO) / CEO / part-time Chairperson (PTC) in Banks – 'Declaration and Undertaking' and allied matters.

directors of banks)[195]. The appointment of senior management requires the RBI's approval (BR Act, s.35B).

Further, the RBI has power to remove any person who is appointed as a chairperson or managing director of a bank and who, in the opinion of the RBI, is not a 'fit and proper' person to hold such office (BR Act, s.10B(6)).[196] )). The RBI also has the power to remove persons at management level under certain circumstances (s. 36AA)[197].

NBFCs

The RBI, for the purpose of considering the application for registration, may require to be satisfied by an inspection of the books of the NBFC that the general character of the management or the proposed management of the NBBC is not prejudicial to the public interest or the interests of its depositors (RBI Act, s. 45-IA (4)). NBFCs are required to perform due diligence for the appointment of directors and the proposed directors are required to provide a declaration attesting there is no criminal case against them (RBI Direction applicable to the sector).[198]

Payment and Settlements Systems

The PSS Act authorises the RBI to assess Payments Systems Operators prior to grating them with authorisation. Regarding Fit and proper, the PSS Regulations details of previous experience of applicant company and associated entities in the payment systems area and sources of finances for executing the payment system project is required to be provided (Chapter 2). However, there are no details on what is required from owners, beneficial owners and managers (e.g., details of criminal proceedings or any other fit and proper issues.) [

FFMC & MTSS

A declaration to the effect that no proceedings has been initiated by / is pending with the Directorate of Enforcement (DoE), Directorate of Revenue Intelligence (DRI) or any other law enforcement authorities, against the applicant company or its directors and that no criminal cases are initiated / pending against the applicant company or its directors is required (Master Direction issued by RBI on Money Changing Activities, s.3; Master Direction on MTSS; para.3.1). However, no such requirements are in place in respect of owners including beneficial owners.

Foreign Exchange Authorised Dealer Category-III

They can only be from select FIs and other institutions who are administered by their respective sectoral regulators (RBI's Master Direction - Money Changing Activities). and are subject to the fit and proper criteria that would be provided by respective sectoral regulators (and any shortcomings they may contain). As noted above for FFMCs and MTSS, the authorisation procedures for these FIs does not require fit and proper tests in the owners and beneficial owners.

Asset Reconstruction Companies

[195] Circular DBOD.No.BC.105/08.139.001/2003-04. 25 June 2004 issued in respect of 'fit and proper' criteria for directors, has laid down specific criteria to be fulfilled by the persons before they are appointed on the Boards of banks. In respect of Public Sector banks, RBI has issued a separate Master Direction DBR.Appt.No: 9/29.67.001/2019-20 dated August 2019, prescribing similar 'fit and proper' criteria for elected directors on the boards of PSBs.

[196] See also RBI circular DBOD.No.BC.105/08.139.001/2003-04 dated 25 June 2004.

[197] The Circumstances are: where the RBI is satisfied that it is in the public interest or for preventing the affairs of a bank being conducted in a manner detrimental to the interests of the depositors or for securing the proper management of any bank it is necessary so to do.

[198] The Non-Banking Financial Company - Systemically Important Non-Deposit taking Company and Deposit taking Company (Reserve Bank) Directions, 2016.

Fit and proper requirements are specified for directors and sponsors (i.e., persons holding at least 10% of the capital) of ARCs, which include self-declarations on convictions (Master Circular on Asset Reconstruction Companies of 10 February 2022; Direction on 'Fit and Proper' Criteria for Sponsors – Asset Reconstruction Companies of 25 October 2018). Transfer of 10% of more shares in an ARC is subject to the RBI's approval, and information is also sought in relation to any other person has beneficial interest in the proposed acquisition (Direction referenced above).

Housing Finance Companies

Fit and proper requirements are specified for directors of and proposed shareholders of HFCs, which include self-declarations on convictions (Master Direction – Non-Banking Financial Company – Housing Finance Company (Reserve Bank) Directions, 2021). There are no requirements in relation to beneficial owners.

Securities Sector

The SEBI (Intermediaries) Regulations, 2008 requires applicants, key management personnel and dominant promoters/ shareholders (promoters or persons holding controlling interest or persons exercising control over the applicant or intermediary, directly or indirectly) to meet "fit and proper" criteria before a grant of registration (Schedule II). This includes information concerning absence of convictions and restraint orders.

Insurance Sector

Applicant, its promoters, investors in insurance companies and directors are subject to fit and proper requirements (IRDAI Registration Regulation, and IRDAI Guidelines on Corporate Governance for insurance companies). The fit and proper criteria include examination of promoter and/or investor's criminal background as well[199].

Transfer of shares in an insurance company are subject to prior approval by the IRDAI (IRDAI Registration Regulation, Schedule 2).

Pension Sector

Sponsor and pension fund must be a 'fit and proper person' as specified which *inter alia* provide financial integrity, absence of convictions or civil liabilities, efficiency and honesty as one of few criteria to be fulfilled by the pension fund and its key managerial personnel (Pension Fund Regulatory and Development Authority (Pension Fund) Regulations, 2015 "Pension fund Regulations"). The applicant, its director, principal officer should not have been black-listed by any regulatory Authority or Government (Central and States) or should not have been convicted of any offence involving moral turpitude or of any economic offences (Pension Fund Regulatory and Development Authority (Central Recordkeeping Agency) Regulations, 2015 – "CRA Regulations". Such requirements also apply to shareholders and beneficial owners of pension institutions PFRDA (Pension Fund) Regulations, 2015, para. 12(j)).

IFSC

In respect of FIs registered in the IFSC, pursuant to s.13(4) of the IFSCA Act, the procedure for registration, recognition, withdrawal of recognition, inspection, investigation etc, all the

[199] Due diligence includes the examination of: (i) insider trading, fraudulent or unfair trade practices or market manipulation by the promoters, investors or group entities; (ii) proceedings including conviction against the entity or any of its promoter or group entities or any of its key management persons, by any regulatory or statutory or judicial bodies in India or outside India; (iii) beneficial ownership of shares of investors or promoters.

provisions as applicable to the FIs under their parent legislation would *mutatis mutandis* apply to the FIs under the IFSC Act. For example, banks which are located in IFSC would be subject to and would be required to comply the same rules and regulations as prescribed by RBI to Banks located elsewhere in India. However, the referenced rules and regulations would be administered by IFSCA under the IFSC Act. As a result, the shortcomings identified in the main legislation would have an impact in the IFSC as well.

***Criterion 26.4 –***

a) India's Financial Sector Assessment Program (FSAP) report was conducted in 2018 by the International Monetary Fund covering the banking sector.[200] Overall, the regulation and supervision of banks was generally compliant or largely compliant with the core principles. Material non-compliance was identified in relation to core principles dealing with independence, accountability, resourcing and legal protection for supervisors; and corporate governance. While the RBI has operational independence in most respects, RBI did not have full discretion to take supervisory actions in relation to public sector banks and there were also legal independence issues (e.g., tenure of RBI's governor). For the securities sector, the evaluation conducted by the International Organization of Securities Commission (IOSCO) in August 2013 concluded that India had fully or broadly implemented the principles that are relevant for AML/CFT.

No FSAP or similar independent assessment has been carried out in related to IFSC core principles institutions, since the IFSC was established in 2019.

Banks, larger UCBs and NBFCs are subject to a ML/TF risk-based supervision. Other core principle FIs are subject to supervision or monitoring that takes into account the ML/TF risk.

b) All other FIs are subject to supervision or monitoring that takes into account ML/TF risks.

***Criterion 26.5 –*** The frequency and intensity of on-site and off-site AML/CFT supervision by the RBI for commercial banks, larger NBFCs and UCBs broadly takes into account:

a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group,

b) the NRA and the ML/TF risks present in India, and

c) the characteristics of the FIs or groups in particular the diversity and number of FIs and the degree of discretion allowed to them under the risk-based approach.

This approach is largely set in RBI's Standard Operating Procedures (SOP) for the Department of Supervision.

For other FIs supervised by the RBI and other FI supervisors, frequency and intensity of supervision is mainly based on the entity's turnover or other prudential consideration but takes into account ML/TF risks to some extent (RBI Guidelines for Inspection of certain authorised foreign exchange dealers; RBI SOP for Oversight of Payment System Operators SEBI Manual for Supervision of Stock Brokers and Depository Participants; SEBI SOP for Inspection of Stock Brokers, Depository Participants and Clearing Members, IRDAI's internal SOP for inspection,

[200] India: Financial Sector Assessment Program-Detailed Assessment of Observance of the Basel Core Principles for Effective Banking Supervision (imf.org).

PFRDA inspection manual for points of presence). The provisions in the relevant manuals and SOPs do not address all aspects of this sub-criteria. There were no equivalent provisions for the IFSC as well as post offices supervised by the Department of Post. Post offices are inspected on an annual basis (Inspection questionnaire).

***Criterion 26.6 –***

Scheduled Commercial Banks, Larger NBFCs, Larger UCBs

RBI reviews the ML/TF risk profile of Scheduled Commercial Banks, Larger NBFCs, Larger UCBs on an annual basis (SOP Department of Supervision). It is not specified if the risk profile is also reviewed when there are major events or developments in the management and operations of the FI or group.

Other NBFCs and UCBs

No framework has been specified.

PSOs

Onsite inspection of PSOs is based on their risk profile (SOP for Oversight of PSOs) and RBI advises that the risk profile of the PSOs is periodically reviewed. It is not specified if the risk profile is also reviewed there are major events or developments in the management and operations of the FI or group.

Authorised Dealers in Foreign exchange

RBI mainly reviews the ML/TF risk profile of FFMC and other authorised dealers upon on-site inspections and some information is also collected offsite. On-site scheduling is mainly triggered based on the entity's turnover but also takes into account ML/TF risks to some extent (Master Regional Office Circular on Guidelines for Inspection of Full Fledged Money changers and non-bank AD Category II (upgraded FFMCs)).

RBI undertakes snap scrutiny, outside the normal inspection cycle, which is essentially updating the risk profile of the authorised dealers in case of any major event. For instance, a snap scrutiny of all MTSS Indian Agents (Money Changers) was taken in 2023 with AML/CFT focus. It is not specified in SOPs or otherwise that the supervisors must review FIs' risk profile at regular intervals and when important events or developments occur.

IFSCA, SEBI, IRDAI and PFRDA

SEBI reviews the risk profile of entities, which take to some extent, account to AML/CFT risks (SEBI's Circular on Policy of Annual Inspection of Members by Stock Exchanges/Clearing Corporations). This has not been clearly established for IFSCA, IRDAI and PFRDA.

It is not specified if the ML/TF risk profile is also reviewed when there are major events or developments in the management and operations of the FI or group.

### *Weighting and Conclusion*

There are gaps for market entry in relation to certain FIs. The fit and proper requirements sometimes do not extend to beneficial owners or are insufficient to identify criminal associations (e.g., for the foreign exchange sector). Whilst supervision is carried out across FI sectors, the application AML/CFT risk-based approach to supervision is not clear for all sectors. Nonetheless, it has been established for most of the banking sector, which is the most material.

**Recommendation 26 is rated Largely Compliant.**

## Recommendation 27 – Powers of supervisors

In its last MER, India was rated largely compliant with former R.29. The following deficiencies were identified: the PMLA did not apply to commodities futures brokers, financial sanctions applied for AML/CFT deficiencies across all sectors were not effective, proportionate or dissuasive; and there was no established supervisory regime covering the banking operations of India Post. The 8th FUR of India noted that the scope deficiency in respect of commodities future brokers had been addressed as a result of the PMLA amendments that came into force in February 2013.

***Criterion 27.1*** – RBI has powers to inspect, call for information and give directions to regulated FIs (BR Act, ss.35, 51 and 56; RBI Act; ss. 45L and 45N; PSS Act, ss.14, 16 and 19; FEMA, ss.11-12). Similar powers are available for other FI supervisors, including India Post (SEBI Act, s.11; IRDA Act, s.14; PFRDA Act, s.14, IFSC Act, ss.13 and 21; NHB Act, s.29A; Government Savings Promotion Act 1873, s.7(A)).

Concurrently, the Director of FIU-IND has powers to enforce compliance with AML/CFT requirements and FI supervisors are empowered and required to assist the Director in the enforcement of the PMLA (PMLA, s.54).

***Criterion 27.2*** – All supervisors have the authority to conduct inspections of FIs (BR Act, ss.35, 45Q and 56; RBI Act; s.45N; PSS Act, ss.14 and 16 and 19; FEMA, s.12; SEBI Act, s.11; IRDA Act, s.14; PFRDA Act, ss.14 and 16, IFSC Act, s.13).

***Criterion 27.3*** – All regulators are empowered to compel production of information relevant to monitoring compliance with the AML/CFT requirements FIs (BR Act, ss.35 and 56; RBI Act; s.45K-L; PSS Act, ss.12-13; FEMA, ss.11-12; SEBI Act, s.11; IRDA Act, s.14; PFRDA Act, s.16, IFSC Act, s.13). In addition, the PMLA has empowered the Director of FIU-IND to compel production of records, discovery and inspection and call for examination of witnesses and documents (s.50). Officers of the respective Regulators are empowered and required to assist the authorities in the enforcement of PMLA (s.54).

***Criterion 27.4*** – Regulators are generally authorised to impose sanctions in line with R.35 for failure to comply with the AML/CFT requirements. This generally includes powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the FI's licence or authorisation (BR Act, ss.22(4)(iii), 36, 36ACA, 46, 47A and 56; RBI Act, ss. 45-IA(6), 58B(4A), 58G; PSS Act, ss.8, 26, 30 and 31; FEMA, ss.10(3), 10(4) and 11(3); SEBI Act, s.15HB; Insurance Act, ss. 3(4) 102, 105; IRDA Act, 14(2)(a); IRDAI(Registration of Insurance Companies) Regulation 2022 , ss 12(2); PFRDA Act, ss.16(7); IFCS Act, s.13(4)(c) read with the parent legislation of each of the FIs).

### *Weighting and Conclusion*

All criteria have been met.

**Recommendation 27 is rated compliant.**

## Recommendation 28 – Regulation and supervision of DNFBPs

In its last MER, India was rated non-compliant with former R.24 because the PMLA did not apply to any of the DNFBP sectors, with the exception of casinos. In addition, with respect to the casino sector the following shortcomings were identified: 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, and lack of dissuasive sanctions for obstructing the regulator's right to inspect.

***Criterion 28.1 –*** A person carrying on activities for playing games of chance for cash or in kind, and associated activities, are considered a casino and therefore a type of DNFBP in India (PMLA, s.2(sa)(i)). Casinos are presently operating only in the States of Goa and Sikkim[201].

a) Casinos are required to be licensed by the State in which they operate.

- *Goa:* The State Government may authorise any game of electronic amusement including slot machines in Five Star Hotels, and table games and gaming on board in vessels offshore (The Goa, Daman and Diu Public Gambling Act, 1976 ("Goa Gambling Act", s.13A).
- *Sikkim:* Casino *games* can only be organised or exhibited with a licence (The Sikkim Electronic Entertainment Games (Control and Tax) Act, 2002 ("Sikkim Games Act"), s.3).

Operating a casino without a licence or authorisation is punishable by a fine of INR 250 (EUR 3) or to imprisonment for any term not exceeding three months (The Public Gambling Act, 1867, s.3).

b) The regulators of casinos have legal or regulatory measures and procedures for licensing of casino for preventing criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, or being an operator of a casino. The regulators conduct vetting processes on the entity and natural persons involving ownership and control including BO of the licensees and continuously review the process for any changes.

c) The Goa Department of Home and Directorate of Sikkim State Lotteries are AML/CFT supervisors in the States and have issued AML/CFT Guidelines for casinos on the basis of PML Rules (s.9(14)(i)), which empower regulators to issue guidelines for implementation of AML/CFT framework (PML Rules 9(14)(i) and 2(1)(fa).

***Criterion 28.2 –*** Rule 2(fa) of the PML Rules defines a regulator as a person or an authority or a government, which is vested with the power to licence, authorise, register, regulate or supervise the activity of REs or the Director as may be notified by the Government for a specific RE or a class of REs or for a specific purpose. In addition, India has issued Notifications under the PMLA in respect of professionals for designation as AML/CFT supervisors. The following authorities are AML/CFT supervisors in the DNFBP sector:

i. Real estate agents and DPMS – Central Board of Indirect Taxes and Customs (PML Rule 2(1)(fa).

ii. Accountants and lawyers – chartered accountants, Institute of Chartered Accountants of India; cost accountants, Institute of Cost Accountants of India (Notification 2045, 9 May 2023). For Lawyers, the regulator is the State Bar Associations (Rule 2(fa) of the PML Rules).

iii. TCSPs – TCSPs that are Company Secretaries are regulated by the Institute of Company Secretaries of India (Notification S.O.2036(E) of 3 May 2023). For other

[201] The Public Gambling Act, 1867 provides a penalty for owning or keeping, or having charge of a gaming-house unless it is not specifically allowed. India indicated that specific prohibition against gambling is contained in laws passed by each State Government. India has shared the legislation of three States detailing this prohibition (Bombay Prevention of Gambling Act, 1887, s.4; Kerala Gambling Act, 1960, s.3; Punjab Public Gambling Act, 1961, s.2). Legislation of other States has not been reviewed.

TCSPs that are not considered other FI/DNFBP in India, the FIU-IND is the AML/CFT supervisor (Rule 2(fa) of the PML Rules).

***Criterion 28.3 –*** CBIC (for real estate and DPMS) and casino supervisors (in Goa and Sikkim) have supervisory measures in place and conducted inspections on the entities under their purview. Professional institutes and the FIU-IND (for TCSPs) were yet to begin supervision activities following their recent designation as AML/CFT supervisors. As a result, no information was available to demonstrate that professionals are subject to systems of compliance with AML/CFT requirements.

***Criterion 28.4 –***

a) The supervisors of DNFBPs derive the power as AML/CFT supervisors through PMLA and its Rule 2(1)(fa) and PMLA Notifications[202] made in respect of professionals (accountants and company secretaries). The regime permits the regulators to use their inherent powers to supervise and monitor compliance with AML/CFT obligations of their respective entities.

b) Measures in place to prevent criminals or their associates from being professionally accredited, or holding a significant or controlling interest, or holding a management function in a DNFBP differ in intensity between sectors, as described below.

- **Accountants:** They need to be registered with their professional organisations.[203] A person shall not be entitled to have his or her name entered in the register if he or she committed an offence involving moral turpitude and punishable with imprisonment or, of an offence, not of a technical nature, committed by him/her in his/her professional capacity.[204]. Those requirements do not address all criminal activity.
- **TCSPs –** TCSPs who are company secretaries are subject to the same requirements described above in relation to accountants.[205] Some TCSPs (e.g., debenture trustees) are required to register with SEBI, and subject to requirements described in R.26. TCSPs that are not registered with SEBI are required to register with FIU-IND. They need to provide information on their corporate structure including details of significant beneficial owners as well as self-declarations stating that there are no proceedings initiated or pending with ED or other LEAs or criminal cases pending against directors/ partners (Guidance for TCSPs for Compliance with PMLA Framework and registration with FIU-IND). It is unclear what checks are performed for owners including beneficial owners of a TCSP firm or checks to identify criminal association.
- **Lawyers –** Lawyers must be admitted by State Bar Councils. A lawyer cannot be admitted if he or she is convicted of an offence involving moral turpitude; or if he or she is convicted of an offence under the provisions of the Untouchability (Offences) Act, 1955. Those requirements do not address all criminal activity. The

[202] Notification S.O.2036(E) of 3 May 2023 and Notification S.O.2135(E) of 9 May 2023.
[203] The Institute of Company Secretaries of India, Institute of Chartered Accounts of India and Institute of Cost Accountants of India, respectively.
[204] The Chartered Accountants Act, 1999, ss.4 and 8; and The Cost Accountants Act, 1959, ss.4 and 8.
[205] The Company Secretaries Act, 1980, ss.4 and 8.

disqualification for enrolment ceases to have an effect after a period of two years from the point of release, dismissal or removal.[206]

- **Notaries** - Notaries must be registered with the Central and State Government. A notary may be removed if he/she has been found to be guilty of misconduct; or is convicted by any court for an offence involving moral turpitude.[207] Those requirements do not address all criminal activity. Whilst there are no specific screening processes for notaries, they are lawyers and subject to requirements referenced above.
- **Real estate agents –** Real estate agents must register with the Real Estate Regulatory Authority in order to trade.[208] Measures to prevent criminals or their associates from being professionally accredited are established at state level. For instance, for the RERA of the State of Maharashtra require applicants for individual or firm registration are required to provide self-certification including details on civil or criminal cases pending against them. Based on the self-certification, Maharashtra RERA obtains performs a background check and request police verification (Rule 11(2)).
- **DPMS –** India applies a combination of mandatory requirements for the DPMS sector as market entry procedures. For DPMS engaged in hallmarking of precious metal jewellery a certification from the Bureau of Indian Standards is required and a jeweller who has been convicted under the provisions of the Bureau of Indian Standards Act, 2016, shall not be eligible to apply for certificate of registration for a cooling period of one year from the date of such conviction (Bureau of Indian Standards (Hallmarking) Regulations, 2018, as per Regulation 7(13)). Those requirements do not address all criminal activity. There are also fit and proper requirements for DPMS engage in import and export transactions Gems and Jewellery Export Promotion Council.

c) The Director of FIU-IND has powers to impose remedial actions and sanctions for contravention of AML/CFT obligations by REs at his own motion or on an application made by a regulator or other authority (PMLA, s.13; see R.35). The monetary penalties imposed by Director of FIU-IND directly correlate to the number of instances of violations identified and may be calibrated depending on the gravity of the offenses, which adds to their proportionality. However, financial penalties may not always be dissuasive, depending on the type of infraction or depending on the size of the RE.

The DNFBP regulators have the authority to impose sanctions inherent in their statutes, but it is not clear if those measures can be taken for non-compliance with AML/CFT obligations.

- ***Casinos***: there is no information on enforcement measures inherent in casino regulators statutes for non-compliance with AML/CFT obligations by casinos.
- ***Accountants and TCSPs (including company secretaries):*** the institutes' disciplinary committee can issue reprimands, remove the name of the profession permanently or temporarily from the register, and issue a fine not exceeding INR 500 000 (EUR 5 590),[209] but it is not clear if those measures can be taken for

[206] The Advocates Act, 1961, s.24-A.
[207] The Notaries Act, 1952, ss. 5, 9 and 10.
[208] The Real Estate (Regulation and Development) Act, 2016, s.9.
[209] The Chartered Accountants Act, 1999, ss.4 and 8; and The Cost Accountants Act, 1959, ss.4 and 8; The Company Secretaries Act, 1980, ss.4 and 8.

non-compliance with AML/CFT obligations. For TCSPs registered with FIU-IND, the FIU Director can cancel registration of TCSPS not fulfilling their PMLA obligations (Guidance for TCSPS for Compliance with PMLA framework and registration with FIU-IND, para.3(i)).

- ***Lawyers, including notaries***: State Bar Associations' disciplinary committee can issue reprimands, suspension or remove the name of the advocate from the State roll of advocates (The Advocates Act, 1961, s.35), but it is not clear if those measures can be taken for non-compliance with AML/CFT obligations.
- ***Real estate agents:*** in case the agent fails to perform its functions including maintaining and preserving such books of account, records and documents as may be prescribed, the Authority may apply a penalty of INR 10 000 (EUR 112) for every day during which such default continues, which may cumulatively extend up to 5% of the cost of plot, apartment or building, as the case may be, of the real estate project, for which the sale or purchase has been facilitated (RERA Act, ss. 62 and 10).

***Criterion 28.5 –***

a) The CBIC (for real estate agents) and casino supervisors have risk assessment tools and supervision procedures for monitoring AML/CFT compliance by the entities. Supervisors of professionals (accountants and company secretaries) and FIU-IND (other TCSPs) are in the process of developing risk-based supervision systems for compliance monitoring following their recent designation as AML/CFT supervisors.

b) The CBIC and casino supervisors have risk rated their entities into high, medium and low for prioritisation of supervision coverage. Since the supervisors of the professionals were yet to set up risk-based supervision capacity, there is no information on application of frequency and intensity of supervision measures.

### *Weighting and Conclusion*

India broadly satisfies the requirements, with moderate deficiencies identified in respect of (i) putting in place procedures for risk-based supervision, (ii) sufficiently preventing criminals and their associates from holding professional accreditation or from holding or being a beneficial owner of a DNFBP firm in some cases and (iii) enforcement particularly on some of the high-risk sectors.

**Recommendation 28 is rated Partially Compliant**

## Recommendation 29 - Financial intelligence units

In its last MER, India was rated largely compliant with former R.26. The main shortcomings were related to the effectiveness issues, namely:

- The dissemination of financial information for investigation or action by the State Police was relatively low in comparison with the State Police's primary responsibility for the investigation and prosecution of TF, predicate offences for money laundering, and for the confiscation of the proceeds of crime.
- Public information released by FIU-IND did not include information on typologies and trends in ML and TF cases as well as related predicate offences.

India amended the Prevention of Money-Laundering Act in 2013 and 2019.

***Criterion 29.1 –***

India established its FIU, the "Financial Intelligence Unit – India" (FIU-IND) via the Office Memorandum (OM) No. 4/10/2004-ES dated November 18, 2004, as the central national agency for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND functions under the statutory basis provided by Chapter IV of the PMLA and PML Rules issued thereunder.

As specified under Rule 8 of the PML Rules, FIU-IND collects reports relating to various prescribed categories of transactions including threshold-based reports (such as cash and cross-border transaction reports) and subjective reports (such as suspicious transaction reports). Further, FIU-IND is empowered under the PMLA to disseminate such reports – and analysis pertaining to them – to concerned law enforcement and security stakeholders.

***Criterion 29.2 –***

a) FIU-IND is the central agency for receiving STRs from reporting entities (PML Rules "Maintenance of records", Rule 2 (1) (g), Rule 3 (1) (D), Rule 8 (2)).

b) The Principal Officer of a reporting entity shall provide information on transactions every month to the FIU-IND Director by the 15th day of the succeeding month, including, inter alia (Rule 3 (1) (A), (B), (BA), (C), (E) (F), Rule 8 (1) (3)):

- all cash transactions of the value of more than INR 1 million or its equivalent in foreign currency (approximately EUR 11 000);
- all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- all cross-border wire transfers of the value of more than INR 500 000 (approximatively EUR 5 600) or its equivalent in foreign currency where either the origin or destination of fund is in India; and
- all purchase and sale by any person of immovable property valued at INR 5 million (approximatively EUR 55 700) or more that is registered by the reporting entity.

***Criterion 29.3 –***

FIU-IND is able to request data from any reporting entities on verification of identity, records of transactions, EDD and any additional information needed for the purpose of performing analysis. The reporting entity must provide the FIU Director with the information within time frame and the manner specified by the Director (Section 12A, PMLA; G.S.R 439 (E), Central Government Gazette Notification dated 1st July 2005 amended by PML Rules "Maintenance of records", Rule 2 (1) (c)).

Every financial institution can be requested to provide additional information, even if it has not been disclosed as an STR or CTR to the FIU. The Director of FIU-IND is empowered to issue warnings, direct compliance and impose sanctions including monetary penalties on the reporting entity for the breach of reporting obligations (Section 13 of the PMLA).

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 (Section 50 of the PMLA).

Various government officers and other functionaries are required to provide necessary assistance to Director of FIU-IND in the enforcement of their statutory functions under the PMLA (Section 54 of PMLA). FIU-IND has access to a wide range of databases and information sources of various authorities including regulators, licensing bodies, and LEAs (see table 3.1 in IO.6). Access is facilitated through a variety of arrangements including Memorandums of Understanding (MoUs) and can be real-time, demand-based, or a mix of the two. FIU-IND has entered into MoUs with partner agencies including the RBI, the MCA, Serious Fraud Investigation Office (SFIO), CBI, ED, NIA, NCB, CBDT, CBIC, SEBI, IRDAI, and CEIB.

In addition to the above, the cross-border currency transfer data related to the Currency Declaration Form (CDF) submitted by international passengers to the Customs department is made available to the FIU by the CBIC (see criteria 32.6).

FIU-IND also has access to Moody's databases RBS (entity KYC details, event details) and ORBIS (organisation details, BO details of private companies).

***Criterion 29.4 –*** FIU-IND's mandate to perform strategic and operational analysis flows from OM No. 4/10/2004-ES dated November 18, 2004. Annexure II to the OM states that the FIU will provide to the specified law enforcement, security and revenue agencies, both general and specific access to financial transaction information it collects. The Annex II provides that the specific access would include referrals of information initiated by FIU-IND that suggest new instances of economic crimes, trends and new modus operandi.

FIU-IND's mandate pertaining to terrorist financing is derived from terrorist financing and other acts of terrorism being predicate offences under the PMLA. As such, the processes and procedures when performing operational and strategic analysis also apply to terrorist financing.

a) The practice of conducting operational analysis commenced in August 2020 as a strategy for identification of STRs for priority analysis and dissemination. Since its commencement, FIU-IND has created a formal structure and mechanism for conducting operational analyses with a standard operating procedure (SOP) for developing operational analysis reports. It uses STR, CTR, CBWTR and NTR data available in FIU-IND's databases – along with other data such as open sources or inputs from partner agencies – to identify persons of Interest; assets; criminal networks; associations and relationships; potential criminality; and to trace proceeds of crime.

b) The mandate for conducting strategic analysis as established under the OM has been formalised and operationalised through internal processes, procedures and workflows. The Strategic Analysis Group (SAG) in the FIU is mandated to undertake analysis of reports filed by reporting entities to identified money-laundering trends and typologies, supported by the Strategic Analysis Lab (see IO.6).

***Criterion 29.5 –*** FIU-IND may disclose upon request or spontaneously information related to any tax, duty or cess (a type of government levy) or to dealings in foreign exchange, or prevention of illicit traffic in the narcotic drugs and psychotropic substances (section 66 (1) (i) of PMLA), and any information received or obtained (Section 66 (1) (ii) of PMLA) by competent authorities within the scope of PMLA. FIU-IND may also provide information under its possession to the relevant agency, if it considers that any other law is being violated (Section 66 (2) of PMLA). Under Section 66(1)(ii), the Central Government is empowered to designate (by executive notification) such other authorities with which FIU-IND's information may be shared. According to the amended G.S.R. No.381(E) dated 27th June 2006, more than 20 different law enforcement, intelligence, and regulatory agencies have been designated under Section 66(1)(ii) including all key LEAs such as the ED, the NIA, the Serious Fraud Investigation Office, the Central Economic

Intelligence Bureau, the Economic Offences Wing of Central Bureau of Investigations, State Police, and key regulators such as the RBI.[210]

The specific authority to disseminate results of operational and strategic analysis is derived from Annexure II to OM No. 4/10/2004-ES dated November 18, 2004, which states that FIU-IND will provide to the specified law enforcement, security and revenue agencies, both general and specific access to financial transaction information it collects. The Annexure II states further that the specific access would include referrals of information initiated by FIU-IND that suggest new instances of economic crimes, trends and new modus operandi. Operational and strategic analysis reports disseminated by FIU-IND to competent authorities essentially convey new instances of economic crimes, trends and modus operandi, along underlying transactional reports.

Annexure II to OM No. 4/10/2004-ES also adds that such authorities shall protect the information against misuse, which may result from an unauthorised access by a third party caused by insecure dissemination.

In pursuance of its mandate, FIU-IND has developed FINNET, a secure channel for two-way communication between the FIU and LEAs. The system is restricted to authenticated and authorised users. Other measures to safeguard communication challenges include end-to-end encryption, automatic blocking of logins after a set number of unsuccessful login attempts, controlled access to content stored on the portal, logging of security incidents, and an Identity Management Solution capable of managing security rights and privileges by individuals. Only nodal officers, designated as such by LEAs, are able to access reports disseminated to them, with a two-factor authentication process.

LEAs also routinely request information through requests made in physical form. Such requests are accepted only from the Nodal Officers of the LEAs, and responses to such requests are also sent in physical form only to the Nodal Officers. Communications with LEAs in physical form are classified as appropriate. MoUs entered into by FIU-IND with LEAs also include explicit provisions on Data Safeguards and Confidentiality.

***Criterion 29.6 –***

a) Access to FIU-IND information is limited (Section 43 of Information Technology Act) and is subject to data protection (Section 43A, 66, 66F of Information Technology Act). FIU-IND has laid down detailed information security policies, in the form of office orders, which include policies, procedures, instructions and templates related to specific domains of information security. FIU-IND information is accessed by the personnel deployed in FIU-IND and LEAs and other government agencies to whom Information is disseminated by FIU-IND.

Access within FIU-IND is regulated by way of internal orders on work allocation and decision-making powers on analysis and dissemination of information; Standard operating procedure pertaining to security in FIU-IND; and information security policies. FIU-IND has established a system for accessing information, analysis and dissemination based on functional, sectoral and

[210] Other competent authorities and departments include the Cabinet Secretariat, Chief Secretaries of State Governments, the Department of Company Affairs, SEBI Insurance Regulatory and Development Authority of India, and other regulators defined under Rule 2 (fa) of the PML Rules (2005), the Director General of Foreign Trade, the Ministry of External Affairs, the Competition Commission of India, the Special Investigation Team at the Ministry of Finance (Department of Revenue), the National Intelligence Grid, the Central Vigilance Commission, the Defence Intelligence Agency, the National Technical Research Organisation, Military Intelligence, the Wild Crime Control Bureau and the Goods and Services Tax Network.

hierarchical differentiation. Further, authority to make final decisions on dissemination of transaction reports and other intelligence products has been allocated to different levels of officers based on the risk/urgency/importance of data in said information/intelligence products.

A standard operating procedure (SOP) has been developed for protection of data and maintaining confidentiality of information disseminated by FIU-IND to LEAs electronically and in hard copy. The SOP has been shared with LEAs.

b) All FIU-IND personnel and information it handles are subject to the Official Secrets Act, 1923 which constitutes India's legal framework for the protection of sensitive government or strategic information. The Act is broad in its scope and prescribes stringent criminal penalties for any breaches of secrecy prejudicial to the security or other interests of the nation.

In addition, FIU-IND personal are subject to a dual-system of confidentiality obligations. Permanent government servants are subject to administrative obligations to maintain confidentiality in the performance of official duties (Rule 3(1)(xx), CCS (Conduct) Rules, 1964 (as updated) the breach of which may attract disciplinary sanctions including dismissal from service. Contracted staff are subject to non-disclosure agreements, which contain equivalent confidentiality and secrecy obligations.

India's Information Technology regulatory framework, as contained in the Information Technology Act, 2000 (as amended), contains both civil and criminal remedies if there is unauthorised access to information, breaches of confidentiality, as well as cyber terrorism and may apply to the FIU.

c) FIU-IND has detailed standard operation procedures for physical security within FIU-IND, which details the manner in which various areas within FIU-IND can be accessed by different classes of personnel, such as employees, support staff and visitors.

The access to FIU facilities and IT-systems is granted only to the authorised personnel.

**Criterion 29.7 –**

a) FIU-IND performs its duties independently and under its own authority as regards the autonomous decisions to request and analyse information on transactions received or obtained from the reporting entities within the prescribed time (Section 12A) and to disseminate information (Section 66). This is explicitly prescribed by the G.S.R. No.439(E) dated July 1st, 2005. Furthermore, the Central Government cannot issue any orders, instructions and directions to require FIU-IND to decide a particular case in a particular manner (Section 52 of PMLA).

b) FIU-IND is able to exchange information with foreign FIUs both on request and spontaneously, on the basis either of bilateral MOUs or an "established relationship".

Section 66 (2) of PMLA authorises the Director of FIU-IND to make their own decision on sharing information or material in their possession with the concerned agency for necessary action. Further, provisions of Annexure II to the OM-4/10/2004-ES enable FIU-IND to establish and maintain relationships with domestic law enforcement, supervisory and regulatory agencies in its capacity of an independent body.

The same OM describes the main/core functions of FIU-IND in relation to the foreign FIUs as follows:

- Screening and processing requests from foreign FIUs;
- Disseminating information to foreign FIUs;
- Establishing and maintaining relationship with foreign FIUs;
- Facilitating, administering and negotiating memoranda of understanding (MOUs) with foreign FIUs.

c) While FIU-IND is attached to the Department of Revenue, it has distinct, statutorily mandated core functions as assigned by the OM No.4/10/2004-ES. FIU-IND also has the status of an independent body reporting to the Economic Intelligence Council chaired by the Minister of Finance.

d) Recruitment to FIU-IND is based on open-applications and involves an assessment of the merits of a candidate by a panel of senior officers (including representatives from outside FIU-IND). Officers from within the government are appointed for specified tenures through the process of deputation, with recruitment conducted by an independent commission.[211] .

All government authorities in India derive their powers to deploy financial resources to carry out their functions, via specific orders related to delegation of financial powers, read with Delegation of Financial Powers Rules, 1978. As such, FIU-IND is an allocated budget, which can be deployed independently for various purposes, in accordance with the schedule of delegated financial powers laid down in the Department of Revenue Office Memorandum (F. No. 15/6/3008-IFU III) dated September 15, 2011, and amendments thereto.

***Criterion 29.8 –*** FIU-IND has been a member of the Egmont Group since May 2007.

### *Weighting and Conclusion*

All criteria have been met.

**Recommendation 29 is rated compliant.**

## Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its last MER, India was rated largely compliant rating with former R.27. The shortcomings were related to the effectiveness issues; India had yet to achieve ML convictions.

***Criterion 30.1 –*** There are designated law enforcement authorities that have responsibility for ensuring that money laundering, associated predicate offences and terrorist financing offences are investigated, within the framework of national AML/CFT policies. The designated LEA for investigating ML offences is the Directorate of Enforcement (Section 49 of the PMLA, Notification of the Government of India of July 1, 2005), for TF crimes – the National Investigation Agency (National Investigation Agency Act, 2008). The associated predicate offences are listed in schedule

[211] The Union Public Service Commission is a dedicated independent commission created under article 315 of the Indian Constitution for recruitment to the Union Government. The Union Public Service Commission is independent from political or other influence under the Constitution through specific provisions pertaining to procedure for appointment and removal of members to said commissions, sanctity of their tenures, and other conditions of service. Apart from government departments, FIU-IND also selects officers from other semi-government organisations (regulators – SEBI, RBI) and contracts employees from public sector banks and other financial institutions, IT and Fintech companies, based on their relevant experience.

to PMLA. These predicate offences are investigated by designated LEAs at both state and federal levels.

***Criterion 30.2*** – LEAs investigating predicate offences, and LEAs investigating terrorist financing, can refer the cases to the ED for ML investigation regardless of the predicate offence that may have occurred. The provisions of PMLA specifically provide for disclosure of information to other law enforcement agencies as well as assistance in investigations (Sections 66 and 54 of PMLA).

State Police can refer their cases to the NIA for investigating TF, especially such cases which have inter-state implications (Section 6 of NIA Act, 2008). When a case is transferred from the State Police to NIA, all investigations of terrorism and terrorist financing are transferred to NIA. The responsibility for TF investigations is shared by State and Centre. State governments initiate cases and conduct investigations. Where cases are complex or have inter-state ramifications, the case is transferred to NIA. If other LEAs uncover a TF angle during investigation, they share information and suspicions with NIA directly.

***Criterion 30.3*** –

The authorities mentioned in 30.1 above, who have been authorised to conduct investigations into suspected predicate, terrorist financing and money laundering offences, have been designated to expeditiously identify, trace, and initiate the freezing and seizing of property (that is, or may become, subject to confiscation) for the respective cases handled by them. However, it is not clear whether or responsibilities for carrying out these actions has been assigned to LEAs.

***Criterion 30.4*** – Authorities which are not LEAs but are responsible for pursuing financial investigations of predicate offences are the tax and customs authorities.

Customs authorities (Central Board of Indirect Taxes & Customs (CBIC)) are responsible to conduct financial investigations of customs (such as smuggling) predicate offences and have powers to expeditiously identify, trace, and initiate freezing and seizing of property according to the Customs Act, 1962, Sections 100 (searches), 104 (arrests), 105 (search premises), 106A (inspection), 107 (examination of persons), 108 (Obligation to furnish information), 110 (seizure of goods, documents and things), etc. The legal basis for referring relevant cases to the ED for ML investigations is provided for in the Customs Act, which identifies the relevant offences as predicate offences for ML (Sections 132 and 135).

According to Section 8 of the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015, Tax authorities (Central Board of Direct Taxes (*CBDT*)) are competent to conduct further actions: (a) discovery and inspection; (b) enforcing the attendance of any person, including any officer of a banking company and examining him on oath; (c) compelling the production of books of account and other documents; and (d) issuing commissions. For the purposes of making any inquiry or investigation, the tax authority is vested with the above-mentioned powers, whether or not any proceedings are pending before it. Any tax authority may, subject to the rules made in this behalf, impound any books of account or other documents produced before it and retain them in its custody for such period as it thinks fit (Section 132 of Income Tax Act, 1961). Section 51 of Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 is predicate offence for ML. This provides the legal basis for referring relevant cases to ED for ML investigations.

***Criterion 30.5*** – The only designated LEA for investigating ML offences is the Directorate of Enforcement (ED), which is not an anti-corruption authority.

CBI is responsible for both investigations of corruption and TF crimes and have sufficient powers to identify, trace, and seizing of assets. According to the section 43F of the Unlawful Activities

(Prevention) Act, 1967 (the UAPA, 1967) the officer investigating any offence under the UAPA, 1967 (including TF related offences), with the prior approval in writing of an officer not below the rank of a Superintendent of Police, may 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 this Act. Under Section 18 of the Prevention of Corruption Act, 1988 (PCA, 1988), a police officer may inspect any bankers books in so far as they relate to the accounts of the persons suspected to have committed that offence or of any other person suspected to be holding money on behalf of such person, and take or cause to be taken certified copies of the relevant entries therefrom, and the bank concerned shall be bound to assist the police officer in the exercise of his powers.

The powers to seize the TF funds are established in Section 25 of the UAPA, 1967, and Section 18A of the PCA, 1988.

### *Weighting and Conclusion*

The only deficiency is that it is not clear whether responsibly for expeditiously identify, trace, and initiate the freezing and seizing of property (that is, or may become, subject to confiscation) has been assigned. However, powers are available (see 4.2a) and practice implies that responsibilities have been assigned (see IO.8).

**Recommendation 30 is rated largely compliant.**

## Recommendation 31 - Powers of law enforcement and investigative authorities

a) In its last MER, India was rated as largely compliant with former R.28. However, the shortcomings were related to the effectiveness issues: India had yet to achieve ML convictions.

***Criterion 31.1*** – The basic powers of law enforcement and investigative authorities are reflected in the ***Code of Criminal Procedure, 1973*** (CrPC). Specific laws (e.g., PMLA) also regulate the application of investigative and procedural actions.

b) Any Court or any officer in charge of a police station who considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the CrPC, a Court may issue a summons or a written order to the person in question, requiring them to produce it at the time and place stated in the summons or order (section 91 of the CrPC).

There are similar provisions for investigations connected with the narcotic drugs and psychotropic substances in section 68E of the Narcotic Drugs and Psychotropic Substances Act, 1985 (the NDPSA, 1985). An officer of a rank not lower than the rank of a Superintendent of Police may inspect and take copies of any entries in a bankers book for any of the purposes of legal proceeding, or may order the bank to prepare and produce, within a time to be specified in the order, certified copies of all such entries, accompanied by a further certificate that no other entries are to be found in the books of the bank relevant to the matters in issue in such proceeding (Sections 6 and 8, Bankers Books Evidence Act, 1891).

Concerning terrorist financing, the officer investigating an offence, with the prior approval in writing of an officer not below the rank of a Superintendent of Police, may 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 Unlawful Activities (Prevention) Act, 1967 (section 43F).

c) Law enforcement and investigative authorities have powers to enable them to conduct searches of persons and premises when investigating (CrPC, Sections 93-101, 165; PMLA, Sections 16-18; UAPA, Sections 43A, 43C; and NDPSA, Sections 41-43, 49,51).

d) Law enforcement and investigative authorities have powers to enable them for taking witness statements (CrPC, Section 161; PMLA, Section 50; NDPSA, Section 68R).

e) Law enforcement and investigative authorities have powers for seizing and obtaining evidence (CrPC, Section 102; PMLA, Sections 5, 16-17, 50, 58; UAPA, Section 43C; and NDPSA, Sections 42-45, 51, 55, 57, 68F).

***Criterion 31.2*** – A number of investigative techniques are at the disposal of competent authorities conducting investigations of TF, ML, and associated predicate offences.

a) There are no explicit provisions for the conduct of undercover operations. At the same time, Section 67 of PMLA and Section 197 of Cr.PC provide immunity to the authorized officers for the actions intended to be done in good faith and for the purpose of discharging their official duty.

b) The Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India (or the Secretary to the Home Department in the case of a State Government) may issue directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 (Rule 419A of the Indian Telegraph Rules, 1951). In 'unavoidable circumstances,' such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been authorised by the Union Home Secretary or the State Home Secretary. Although the notion of unavoidable circumstances appears to be vague, case studies have demonstrated that this investigative technique is at the disposal of the investigating officer.

c) The Central Government may, for the purposes of enhancing cyber security and for the identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource (Section 69B, Information Technology Act 2000).

Under Information Technology (Procedure and safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, Secretary (Department of Telecom) has the powers to allow lawful interception of aural or other acquisition of the contents of any information through the use of any intercepting device, viewing examination or inspection of the contents of any direct or indirect information and diversion of any direct or indirect information from its intended direction to any other direction. In special cases an officer not below the rank of Joint Secretary may also allow legal interception.

d) According to the Section 50A of the NDPSA, 1985, the Director General of Narcotics Control Bureau or any other officer authorised by him in this behalf, may undertake controlled delivery of any consignment to (a) any destination

in India; (b) a foreign country, in consultation with the competent authority of such foreign country to which such consignment is destined.

Controlled delivery may also be undertaken by the Customs authorities by an officer authorised by the Principal Additional Director General/ Additional Director General of Directorate of Revenue Intelligence (Section 109A of the Customs Act, 1962; Controlled Delivery (Customs) Regulations, 2022). The list of goods for which controlled delivery can be undertaken are also specified in the Controlled Delivery (Customs) Regulations, 2022. This includes narcotics, precious stones and metals, currency and negotiable instruments, etc. Such controlled delivery can be undertaken to any destination within India, or to a foreign country in consultation with the competent authority of that country.

***Criterion 31.3 –***

Indian law regulates legal mechanisms for identifying accounts held or controlled by natural or legal persons, and ensures that competent authorities have a procedure to identify assets without prior notice to the owner.

a) In addition to the powers of law enforcement and investigative authorities described in Criterion 31.1(a), India has also created the Central KYC Registry (CKYCR). The main objective of CKYCR is to operate as a repository for KYC records across all financial sector entities in India. Each account (across financial institutions) pertaining to a natural or legal person would be linked by a common KYC identifier. CYKC Register maintains basic and profile information of all account holders, along with copies of KYC documents submitted. Submission of KYC information is required for all bank accounts opened after 2017. In addition, when a bank account (created before 2017) is subject to repeated KYC, at prescribed intervals, the same information will also be added to the CKYCR. LEAs use their powers to access the registry (Section 91 of CrPC). In addition, CKYCR being a reporting entity under the PML Rules (Rule 2 (1) (ac)), the specific KYC information is available to FIU-IND in accordance with the PML Rules.

b) The CKYCR, property registrars, as well as FIs, DNFBs and VASPs are all reporting entities under the PMLA (Sections 2(1) (wa) and 2 (1) (sa) of PMLA) which empowers the FIU-IND to request any information from them (Sections 12 and 12A, PMLA). The same provisions expressly require that every information provided to the FIU-IND be kept confidential thus preventing prior notification to the 3rd parties (i.e., clients or owners of assets). In turn, competent authorities can seek information from FIU-IND (Section 66, PMLA).

***Criterion 31.4 –*** There is no direct indication in the laws that LEAs can request information from the FIU, but this can be inferred from an interpretation of the CrPC, PMLA and other laws. This has also been demonstrated in practice.

Under Section 91 of the CrPC any Court or any officer in charge of a police station can request documents and things from the person whose possession or power such document or thing is, when it is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the CrPC.

According to the Section 66 of the PMLA and Notification of the Government of India of July 1, 2005, the Director of FIU or any other authority specified by him by a general or special order in this behalf may furnish or cause to be provided to:

- any officer, authority or body performing any functions under any law relating to imposition of any tax, duty or cess or to dealings in foreign exchange, or prevention of

illicit traffic in the narcotic drugs and psychotropic substances under the Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985); or

- such other officer, authority or body performing functions under any other law as the Central Government may, if in its opinion it is necessary so to do in the public interest, specify, by notification in the Official Gazette, in this behalf, any information received or obtained by such Director or any other authority, specified by him in the performance of their functions under this Act, as may, in the opinion of the Director or the other authority, so specified by him, be necessary for the purpose of the officer, authority or body specified in clause (i) or clause (ii) to perform his or its functions under that law.

### *Weighting and Conclusion*

India meets all of the criteria, with the exception that it does not have specific provisions for conducting undercover operations apart from a general waiver of responsibility of an officer acting in good faith.

**Recommendation 31 is rated largely compliant.**

## Recommendation 32 – Cash Couriers

India was rated partially compliant with the former SR.IX in its 2010 MER. The deficiencies related to limitations in the cross-border declaration/disclosure systems appearing to only apply to movements of currency and BNI via airports and not through land borders, mail or cargo.

***Criterion 32.1 –*** India uses a declaration system for incoming cross-border transportation of currency and BNIs, requiring the completion of a Currency Declaration Form (CDF) [Foreign Exchange Management (Export and Import of Currency) Regulations, 2015]. For outgoing cross-border transportation of currency and BNIs by travellers, India utilises a disclosure system for passengers carrying currency and BNI below a threshold of USD 3 000. Movement of foreign currency and BNIs through mail and cargo is prohibited with few exceptions [Regulation 3 and Regulation 7 of the Foreign Exchange Management (Export and Import of Currency) Regulations, 2015]. Export of currency and BNIs is only permitted in certain cases and India relies on targeted intervention by Customs authorities on the basis of intelligence or the formation of suspicion to ensure compliance with a disclosure obligation. For export of currency through couriers, mail and cargo, exporters are required to file a shipping bill, or other form as prescribed by Regulations [Courier Imports and Exports (Electronic Declaration And Processing) Regulations, 2010; Exports by Post Regulations, 2018].

***Criterion 32.2 –*** India uses a declaration system for the incoming physical transportation of currency or BNIs. Travellers are required to complete the CDF when bringing in foreign currency notes exceeding USD 5,000 or when the aggregate value of all forms of foreign currency, including notes and traveller's cheques exceeds USD 10,000 [Section 6, Foreign Exchange Management (Export and import of currency) Regulations, 2015]. Travellers are also restricted from importing or exporting Indian currency exceeding INR 25 000 (USD 305) per person [FEM Rules 2015]. As part of this prohibition, there are no declaration requirements for exceeding this threshold and any Indian currency above this amount is seized upon detection.

Declarations for movement of currency through mail or cargo are completed in the prescribed forms, such as Shipping Bills [Courier Imports and Exports (Electronic Declaration and Processing) Regulations, 2010; Exports by Post Regulations, 2018].

***Criterion 32.3 –*** India uses a disclosure system for the export of currency. India imposes a threshold on the amount of foreign currency which may be taken out of India of USD 3 000, but permits any foreign currency obtained by the traveller through purchase from an authorised dealer to be transported across India's borders. The disclosure obligations only apply when enquiries are made by Customs officials upon a traveller's exit from India. Upon inquiry, travellers are required to provide authorities with a 'cash memo' which may be requested when purchasing foreign currency in India from authorised dealers or a copy of the CDF completed upon arrival into India [Section V, FED Master Direction No.3/2015-16]. This is considered sufficient to constitute the equivalent of a truthful declaration.

***Criterion 32.4 –*** Customs officers have the power to summon persons to give evidence and produce documents to provide further information on the origin of the currency or BNI and its intended use [Section 108, Customs Act]. Powers are also given to Customs officers in relation to search, seizure and arrest [Chapter XIII of the Customs Act]. The Central Government is also empowered to confer enforcement powers to customs officers, police officers, central excise officers or any other officer to enforce currency control powers [Section 38 of the Foreign Exchange Management Act ('FEMA').

***Criterion 32.5 –*** India has proportionate and dissuasive sanctions available for false declarations and disclosures. False declarations are considered a predicate offence under the PMLA and punishable by a maximum penalty of 2 years' imprisonment and a fine [Sections 132 and 135 of the Customs Act]. The monetary fine for false declarations and disclosures can extend to five times the value of the currency [Section 114AA, Customs Act]. Sanctions in the form of monetary penalties of up to three times the value of the foreign currency and imprisonment of up to 5 years for natural persons [Section 13, FEMR]. Sanctions can also be extended to a director, manager, secretary or other officer of a company should the false declaration or disclosure be committed by that company [Section 42, FEMR]. Habitual offenders may be subject to preventive detention to prevent future offending [Section 3, Conservation of Foreign Exchange and Prevention of Smuggling Activities (COFEPOSA) Act, 1974].

***Criterion 32.6 –*** Information obtained through the declaration process in the form of CDFs is made available to FIU through MFTP file transfers on a monthly basis. This information is then integrated with the FIU's data holdings. Disclosures are not recorded by Customs officials. However, when a search of a person and/or their belongings is conducted, a record of this is created and may be made available to the FIU.

In addition, the FIU may also be notified of suspicious cross-border incidents by Customs officials under the information sharing agreement between FIU-IND and Customs but there is no explicit requirement to do so.

***Criterion 32.7 –*** India has adequate domestic coordination mechanisms in place to ensure customs, immigration, AIU of Income Tax, CISF, CBI, and other related authorities coordinate on matters related to cash couriers. In addition to the exchange of information between Customs and FIU-IND, regular coordination meetings are conducted between border agencies and the Advance Passenger Information System serves to share information and enhance coordination across agencies at ports of entry/exit. Every port of entry has its own coordination mechanism across the various border agencies monitored by the authority in administrative charge of the port.

**Criterion 32.8 –**

**Criterion 32.8 (a)** Customs Officials are empowered to stop and search when there is a suspicion of ML/TF or a predicate offence in certain instances. Where currency or BNI above the threshold is identified as part of this search, Customs Officials are able to restrain this currency/BNI under the powers enshrined in the Customs Act. For currency and BNI identified

during this search which is below the threshold, Customs coordinate with ED to exercise the powers \, and with respective LEAs to restrain the currency or BNI [Section 54 of PMLA]. Customs officers are not able to utilise *suo moto* the provisions of the PMLA, but are required to assist ED officers.

***Criterion 32.8 (b)*** Competent authorities in India are able to seize goods above the prescribed limits for a reasonable time when there is a false declaration or disclosure [Section 110 of the Customs Act]. Customs Officers are empowered to search and screen persons, premises and conveyances [Sections 100-103, 105 and 106 of the Customs Act]. The definition of 'goods' includes currency and BNIs [Section 2(22) of the Customs Act].

***Criterion 32.9*** –

Customs has in place a range of international cooperation arrangements with other customs authorities abroad. India has entered into 34 Agreements on Cooperation and Mutual Administrative Assistance in Customs matters (CMAA) with 63 different countries/regional groups. These agreements cover provisions relating to the exchange of information for the proper application of Customs law and for prevention, investigation and combating of Customs offences.

The information retained through the declaration system allows for international cooperation and assistance under these agreements, in accordance with R.36 to 40. As detailed in c.32.7, to facilitate such cooperation, information collected through the CDF, including information where the threshold has been exceeded, value of currency/BNIs and the passport details of the individual, is retained by the Customs Authorities and is made available to FIU-IND through monthly file transfers and retained indefinitely. Information regarding false declarations and suspicion of ML/TF, and related enforcement actions, are shared through the coordination mechanisms at each port. This information is retained on the Customs central server and made accessible to the FIU, or upon request, for the purposes of international cooperation.

As per c.32.6, records of searches related to disclosures are retained on the Customs central server and can be accessed for the purposes of international cooperation. This does not extend to disclosures where a search is not conducted.

***Criterion 32.10 –*** Information collected through India's declaration system and the limited information collected in the disclosure system is obtained lawfully, fairly used and is audited on a yearly basis. This information is considered transactional and is managed according to the data sharing policy under CBIC's procedures relating to transactional data. Unauthorised publication of this information is an offence [Section 135AA of the Customs Act]. These safeguards do not limit the movement of capital, nor unreasonably restrict legitimate trade payments.

***Criterion 32.11 –*** India subjects natural and legal persons who are carrying out the physical cross-border transportation of currency or BNIs related to ML/TF, or predicate offences, to proportionate and dissuasive sanctions and confiscation measures. The range of sanctions extend up to seven years imprisonment and/or an unlimited fine for duty evasion and confiscation action is possible as duty evasion represents a predicate for ML [Sections 132 and 135, Customs Act; Sections A and B, PMLA]. Imprisonment of up to two years and/or an unlimited fine are available for submitting a false declaration or using a false document in the process.

The offence of holding the proceeds of terrorism also extends to a person undertaking physical cross-border transportation of funds linked to terrorism [Section 21 of the UAPA]. This is punishable via a maximum penalty of life imprisonment and an unlimited fine, with liability extended to a promoter, director, manager, secretary or other officer of a company where the offence is committed by that company [Section 22A of UAPA].

### *Weighting and Conclusion*

India has implemented a generally comprehensive declaration system for incoming cross-border movements, with minor deficiencies on information collected, retained or shared for the purposes of domestic coordination and international cooperation under the disclosure system for outgoing cross-border movements.

**Recommendation 32 is rated largely compliant.**

## Recommendation 33 – Statistics

In its previous MER, India was largely compliant with R.32 as no statistics were available regarding the number of currency declaration forms collected at Land Customs Stations, and detections of smuggling of currency and BNI through the mail and containerised cargo.

***Criterion 33.1 –***

a) STRs, received and disseminated

The process of receipt, analysis and dissemination of financial intelligence is conducted electronically. All STRs are submitted by REs through the FINNET portal of FIU-IND. Following submission, these STRs are then processed and linked to all relevant reports available in the database using rules of identity and relationship resolution. Comprehensive statistics of STRs received and disseminated are maintained on a real time basis; enabling statistics on STRs received and disseminated to be generated from the system at any point of time. Yearly statistics are also published in Annual Reports of FIU-India, which are available on FIU-India's website.

b) ML/TF investigations, prosecutions and convictions

The statistics shared by ED captures the number of pending ML cases, number of new cases recorded, number of cases closed and details of trials under the PMLA.

The ED maintains statistics with respect to ML investigations, prosecutions and convictions. ED has developed a web-based application namely MPR (Monthly Progress Report) to enter and consolidate statistics relating to PMLA cases.

In respect of TF investigation, prosecutions and convictions, comprehensive statistics are available on an online application called integrated Module on Terrorism (i-MoT).

c) Property frozen; seized and confiscated

The information of seizures and confiscation are maintained by the respective authority that conducts these. For example, seizures and confiscation data under the PMLA is maintained by the Enforcement Directorate. Further, the 'Competent Authority & Administrator' maintains and reports property subject to seizure orders and confiscation orders to the Ministry of Finance.

d) Comprehensive information on prop frozen seized–and confiscated is available from an online application called integrated Module on Terrorism (i-MoT).

e) MLA and other international requests

Statistics on incoming and outgoing requests for international cooperation, both formal and informal, made to regulators and LEAs are maintained by the central authority.

### *Weighting and Conclusion*

**Recommendation 33 is rated Compliant.**

## Recommendation 34 – Guidance and feedback

In its last MER, India was rated partially compliant with former R.25. Deficiencies related to written guidance provided to the casino sector to assist with the implementation of the PML rules being limited in scope.

***Criterion 34.1 –***

Guidance and feedback by supervisors

PMLA

Rules requires regulators to issue guidelines incorporating the CDD requirements established in the Rules (Rule 9(14)).

FIs

FI regulators have issued directions/circulars/guidelines on preventive measures for AML/CFT. They have established mechanisms to provide feedback to FIs, mostly following on-site inspections or via outreach programs. Commercial banks have also an assigned contact point in RBI's department of supervision. In addition, some regulators such as the RBI and IRDAI provide regular training to FIs on AML/CFT aspects.

DNFBPs:

Guidance has been provided for most DNFBP sectors covering different aspects of preventive measures and feedback channels were established, mainly through outreach programs. This includes guidelines covering AML/CFT obligations as well as detection and filing of STRs for the recently notified TCSPs. Guidance has not yet been issued for lawyers including notaries.

In addition, FIU-IND has issued guidelines to REs for filing of various reports (STRs, cross border wire transfer reports) and on red flag indicators for FIs (banks, market intermediaries, credit card operators, insurance companies, MTSS operators, payment intermediaries). FIU-IND also issued typology-based guidance (e.g., on TF, on TF, shell companies and TBML) to REs sharing insights from operational analysis and feedback received from LEAs on STRs. It also provides feedback to REs time to time on usefulness of STRs.

### *Weighting and Conclusion*

Guidance and feedback mechanisms are available for most sectors, except for lawyers including notaries.

**Recommendation 34 is rated Largely Complaint.**

## Recommendation 35 – Sanctions

In its last MER, India was rated partially compliant with former R.17. Sanctions applied for AML/CFT deficiencies across all sectors were not effective, proportionate or dissuasive and the PMLA did not apply to commodities futures brokers. India's 8th FUR concluded that the country had taken measures to improve compliance with that Recommendation, which could then be considered essentially equivalent to largely compliant.

***Criterion 35.1 –***

R.6 - TFS

FIs which violate TFS obligations can face proportionate and dissuasive administrative penalties under their respective regulations (see below).

Where there is indication of sufficient knowledge or participation into violation of TFS, the UAPA penalties would apply which are proportionate and dissuasive.

As noted under R.6 and R.7, there is no specific penalty available for DNFBPs as well as natural and legal persons except under their TF laws.

R.8 – NPOs

Under the ITA, non-compliance with obligations is usually addressed through the cancellation of the NPO's registration under section 12AB ITA and/or imposing a range of taxes where tax would have otherwise been exempted. This includes in situations where statements are not maintained or audited. Under the state legislation relating to the Societies Registration Act, Charities Commission of the respective states have investigative powers into the affairs of societies in their state, as well as access to a broader range of criminal and administrative sanctions against breaches under their legislation, which includes the ability to pursue criminal prosecution against every person (including promoter of company or trust or settlor of the trust) who at the time of the offence was either in charge or responsible for the conduct of the as well as to sanction or dissolve non-functioning NPOs.

R.9 to 23 - Administrative sanctions (FIs, VASPs, DNFBPs)

The Director of FIU-IND may, either of his own motion or on an application made by any authority (PMLA, s.13(2)):

a) issue a warning in writing; or

b) direct a RE (FI, VASP or DNFBP) or its designated director or employees, to comply with specific instructions; or

c) direct a RE or its designated director or employees, to send reports on the measures it is taking; or

d) impose a monetary penalty on a RE or its designated director or employees, which shall not be less than INR 10 000 (EUR 111) but may extend to INR 100 000 (EUR 1113) for each failure.

The monetary penalties imposed by Director of FIU-IND directly correlate to the number of infractions identified and may be calibrated depending on the gravity of the offenses, which adds to their proportionality. However, financial penalties may not always be dissuasive, depending on the type of infraction or depending on the size of the institution. For instance, if there has been tipping off concerning the filing of an STR – whilst this one offense is serious, a maximum penalty of EUR 1113 would be applied which would not be dissuasive. The sanctions can lead to more significant amounts even there are multiple failures.

In addition to the sanctions imposed the Director of FIU-IND, FI Regulators are generally authorised to impose sanctions for failure to comply with the AML/CFT requirements. This generally includes powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the FI's licence or authorisation (BR Act, ss.22(4)(iii), 36, 36ACA, 46, 47A and 56; RBI Act, ss. 45-IA(6), 58B(4A), 58G; PSS Act, ss.8, 26, 30 and 31; FEMA, ss.10(3), 10(4) and 11(3); SEBI Act, s.15HB; Insurance Act, ss. 3(4) 102, 105; IRDA Act, 14(2)(a); IRDAI (Registration of Insurance Companies) Regulation 2022, ss 12(2); PFRDA Act, ss. 27(4), 28 and 50; IFCS Act, s.13(4)(c) read with the parent legislation of each of the FIs). FI Regulators can also impose a range of sanctions for lack of compliance with directions:

e) **Banks:** RBI can impose fines up to INR 10 million (EUR 111 317) and where a contravention or default is a continuing one, a further fine up to INR 100 000 (EUR 1113) for every day during which the contravention or default continues

(BR Act, ss.46(4) and 47A).[212] The RBI can also impose sanctions for failure to produce accounts, documents or statements (up to INR 2 million (EUR 22 000), and addition INR 50 000 (EUR 548) daily fine, as per s. 47A(2)) and sanctions for producing false statements or wilful omissions (imprisonment of up three years or fine up to INR 10 million (EUR 110 000) or both per s. 47A(1)). The financial sanctions, if imposed on their own, do not appear to be dissuasive for banking institutions; however, if they are accompanied by measures such as business restrictions, this may lead to a more dissuasive effect.

f) **Non-banking financial companies**: RBI can impose fines up to INR 100 000 (EUR 1113) and where a contravention or default is a continuing one, a **further** fine of up to INR 10 000 (EUR111) for every day of default after the first (RBI Act, s.58B(6)). These financial sanctions, if applied on their own, are not dissuasive.

g) **Foreign exchange dealers**: RBI can impose fines up to INR 10 000 (EUR 111) and where a contravention is a continuing one, with further fine which may extend to INR 2 000 (EUR 22) for every day during which such contravention continues (FEMA, s.11(3)). These financial sanctions, if applied on their own, are not dissuasive.

h) **Payment System Operators:** RBI can impose monetary penalty on authorised PSOs not exceeding INR 500 000 (EUR 5 565) or twice the amount involved in such contravention or default where such amount is quantifiable, whichever is more, and where such contravention or default is a continuing one, a further penalty up to INR 25 000 (EUR 278) for every day in which the contravention or default continue (PSS Act, ss.26 and 30). These financial sanctions, if applied on their own, are not dissuasive. The RBI is also empowered to revoke the PSO authorisation, if the PSO contravenes fails to comply with its orders/ directions (PSS Act, s.8).

i) **Securities sector**: SEBI can impose fines ranging from INR 100 000 (EUR 1113) to INR 10 million (EUR 111 317) (SEBI Act, s. 15HB). These financial sanctions may not be dissuasive for larger businesses.

j) **Insurance sector**: IRDAI can impose fines ranging from INR 100 000 (EUR 1113) to INR 10 million (EUR 111 317) (Insurance Act, s.102). These financial sanctions may not be dissuasive for larger businesses. Regulation 12(2) of IRDAI Regulations 2022 states that registration of any insurer can be cancelled if the insurer defaults in complying with any requirement of PMLA.

k) **Pension sector**: PFRDA can impose fines up to INR 10 million (EUR 111 317) or five times the amount of profits made or losses avoided, whichever is higher (PFRDA Act, s.28).

l) **IFSC entities**: The IFSCA can exercise all powers exercisable by an appropriate regulator under the respective Act (such as RBI, SEBI, IRDAI, PFRDA which are

[212] However, the RBI cannot impose penalties to a banking company, where any complaint has been filed against that banking company in any court in respect of an offense of a similar nature to the one RBI would impose penalties to (BR Act, s.47A(7)). Similarly, the BR Act prohibits action against a banking company in any court of law in relation to a contravention in respect of which a penalty has been imposed by the RBI under section 47A (BR Act, s.47A(4)).

specified in First Schedule of the IFSCA Act) (IFSCA Act, s.13). Therefore, IFSC could apply the same sanctions described above in the case of similar failures.

m) **Department of Posts**: In addition to the PMLA (see above), the DoP has also power to impose sanctions against officials for failure to comply with AML/CFT requirements, (CCS (CCA) Rules 1965).

For DNFBPs, sanctions powers inherent to the statutes of DNFBP regulators are described in Recommendation 28 (c.28.4.c); however, as noted there, it is unclear if these sanctions could be applied for non-compliance with AML/CFT obligations. PMLA sanctions apply, nonetheless.

For VASPs, PMLA sanctions apply (see Recommendation 15, c.15.8), and the FIU-IND also has the power to cancel registration of a VASP that fails to comply with PMLA requirements.

Criterion 35.2 –

**R.6 – TFS**

For FIs and DNFBPs, see below.

**R.8 – NPOs**

The prescribed punishments under the ITA and respective Societies Registration Act apply to anyone either in charge or responsible for the conduct.

R.9 to 23

Under the PMLA, monetary sanctions are applicable both to REs and designated directors or employees, where in the course of any inquiry, the Director finds that a RE or its designated director or any of its employees has failed to comply with CDD and other obligations imposed (PMLA, s.13(2)). In addition, where a contravention of any of the provisions of PMLA, PML Rules or directions has been committed by a RE 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 is also considered liable for the contravention (PMLA, s.70).

RBI sanctions do not apply to officers of the Central Government or the RBI that have been nominated or appointed as directors of public sector banks, or to officers of public sector banks that have been nominated or appointed as director of any other public or private sector bank (BR, s. 51(1)(c). Public servant directors would, nonetheless, be subject to the Indian Penal Code (e.g., section 166 of IPC (Public servant disobeying law, with intent to cause injury to any person), section 167 (Public servant framing an incorrect document with intent to cause injury)).

### *Weighting and Conclusion*

Overall, India has measures in place to apply sanctions for non-compliance with AML/CFT measures. They are generally proportionate but not always dissuasive, depending on the type of infraction or size of the institution. However, many regulators also have the powers to withdraw, restrict or suspend the licences or authorisations, and those add to the overall dissuasiveness of the regime. There is no specific penalty available for breaches of TFS obligations for DNFBPs as well as natural and legal persons, apart from the TF offence where there is indication of sufficient knowledge or participation into violation of TFS, although for FIs, there are administrative penalties under their respective regulations.

**Recommendation 35 is rated Largely Complaint.**

## Recommendation 36 – International instruments

In its 2010 MER, India was rated partially compliant with former R.35 and partially compliant with SR.I. The main deficiencies were that the Palermo Convention had not been ratified and that ML/TF provisions required amendment to fully implement the relevant Conventions. Since the adoption of its MER in 2010, India made a number of amendments to its AML/CFT regime and the 2013 FUR found the level of compliance with former R. 35 and SR.I to be essentially equivalent to LC.

***Criterion 36.1 –*** India ratified the Vienna Convention on 27 March 1990, the Palermo Convention on 5 May 2011, the UN Convention against Corruption (the Merida Convention) on 9 May 2011, and the Terrorist Financing Convention on 22 April 2003.

***Criterion 36.2 –*** Consideration of India's implementation of the relevant international instruments is determined by the assessment of India's compliance with the relevant FATF Recommendations that cover the various articles.

The relevant articles of the Vienna, Palermo and Merida Conventions are implemented through the PMLA and Criminal Procedure Code. This includes the conduct of concealment, acquisition, possession and use of criminal proceeds [Section 3 of PMLA]. Article 5 of the Vienna Convention and Article 12 of the TOC Convention are covered under the Indian the seizure/confiscation regime of the laundered proceeds [Sections 8, 58B and 60 of the PMLA; Sections 105A, 105C, 105E, 105K, 105L of the Cr.PC]. The amounts of fines imposable on legal persons for the ML offence are not specified, however, the average fine imposed for ML convictions between 2017 and 2023 is INR 1.05 million (EUR 11,667) ranging from INR 5 000 (EU56) to INR 20 million (EUR222,222) which appear effective, proportionate and dissuasive [Section 4 of PMLA].

India primarily implements the TF Convention through the UAPA. The financing of the offences falling within the scope of the Treaties annexed to the TF Convention are criminalised and all relevant offences are covered in accordance with Art. 2.1(a) of the TF Convention [Section 15(2) and Schedule 2 of the UAPA].

The threat to international organisations in accordance with Art. 2.1(b) of the TF Convention and attempt to finance terrorism in accordance with Art. 2.4 of the TF Convention are criminalised [Section 15(1)(c); Section 17 of UAPA]. Confiscation of funds to be used by terrorist individuals in accordance with Art. 8 of the TF Convention is also included [Section 2(g) of UAPA].

### *Weighting and Conclusion*

**Recommendation 36 is rated compliant.**

## Recommendation 37 - Mutual legal assistance

In its 2010 MER, India was rated largely compliant for R.36 and SR.V. In both cases it was stated that MLA in coercive actions might be hampered as a result of domestic legal deficiencies (dual criminality).

***Criterion 37.1 –*** Mutual legal assistance relating to criminal matters including predicate offences can be provided to foreign countries under the provisions of the Criminal Procedure Code (Cr.PC), which is the underlying criminal law of India. India can provide a wide range of assistance in tracing, identifying, attaching, seizing and forfeiture of property, if a request in this regard is received from a jurisdiction with which there exists a bilateral or multilateral treaty or on the basis of reciprocity [Sections 105A to 105L of the Cr.PC]. Where a Court in India receives a request for service or execution of a summons/warrant from a Court, Judge or Magistrate in a

contracting State, it shall cause the same to be served or executed as if it were a summons or warrant received by it from another Court within its local jurisdiction [Section 105(2) of Cr. PC]. A Letter of Request from a country or place outside India can also be executed and referred to a Court or an authority for investigation in India [Section 166B of Cr. PC].

The Central Government can conclude agreements with foreign countries for enforcing the provisions of various domestic laws including PMLA, for exchange of information in investigation of offences and for exchange of information for prevention of any offence under PMLA or under the corresponding law in force in that country [Section 56 of the PMLA]. India has entered into Mutual Legal Assistance Treaties or Agreements with 46 countries, out of which 40 MLATs have been ratified.

The Ministry of Home Affairs (MHA) Guidelines dated 4th December 2019 provide comprehensive guidance in respect of procedures to be followed for Mutual Legal Assistance, requiring these requests to be dealt with 'promptly' [paragraph 1.10 (vi) of the MHA Guidelines].

***Criterion 37.2 –*** The MHA Guidelines establishes the procedure for executing incoming requests for MLA in keeping with the relevant legislation on international cooperation [Section 166B8, Section 105K9 and Chapter VII A of CrPC, Section 5810 and Section 6111 of PMLA]. All the requests to India for the mutual legal assistance in criminal matters are made to the Central Authority which is the MHA. The requests received through diplomatic channels by Ministry of External Affairs (MEA) i.e., Territorial Division, CPV Division, etc., are also forwarded to IS-II Division, MHA. After receiving the request, the Central Authority of India examines whether the request is complete and fit to be executed in India. While deciding about the execution of request, the Central Authority of India can seek the assistance of MEA and other relevant enforcement agencies in India including JD (TFC), CBI to help determine whether it should be executed or not (TFC), CBI. [Part II C. para 2.2 of the MHA Guidelines].

In case the request is found to be fit for execution, the Central Authority sends it for execution through Assistant Director (AD) of the International Police Cooperation Unit (IPCU), Central Bureau of Investigation (CBI) to the Interpol Liaison Officers (ILO), of State/UTs or the law enforcement authority concerned. CBI and each LEA has its own documented processes for timely prioritisation and execution of MLARs. Standard Operating Procedures (SOPs) on executing MLA requests were issued by the Central Bureau of Investigation in July 2023 to streamline the execution of such requests. These SOPs establish some guidelines for prompt action and the requirement for monthly reviews of all pending requests, with each branch to establish a mechanism to oversee the execution of requests. Whenever the Central Authority of India decides that the request should be refused or postponed, it is required to promptly inform the Requesting Country [Part II C. para 2.3 of the MHA Guidelines].

All the incoming requests are executed in terms of the provisions of extant Bilateral Treaties or Agreements, Multilateral Treaties or Agreements or International Convention and in accordance with Indian Laws [Part II C. para 2.4 of the of the MHA Guidelines].

Further, the MHA Guidelines provide for the monitoring process. AD (IPCU), CBI provide the complete details of the execution of request to IS-II Division, MHA in the format provided below in the last week of every month or earlier, as required by IS-II Division, MHA. [para 2.5 of Part D of the MHA Guidelines].

On a quarterly basis, IS-II Division, MHA along with officers of AD (IPCU), CBI, ED and NIA review the compilation of data and progress of execution of requests [para 2.6 of Part D of the MHA Guidelines]. A biannual meeting of ILO's concerned takes place for analysing the progress of execution and issues faced in making the requests [para 2.7 of Part D of the MHA Guidelines].

***Criterion 37.3 –*** No conditions under which a request would be refused are provided in legislation. It is at the discretion of the Central Government whether to pass a request on to the CBI or other LEAs, but that discretion must be exercised if it thinks fit in accordance with the PMLA or other laws, and in keeping with the specialisation of the relevant LEA [Section 166B of the Cr.PC; Section 58 of PMLA]. This discretion does not impose any additional grounds for refusal. Otherwise, any conditions that are imposed would be contained in the MLAT itself.

The request for assistance is generally refused if:

a) the execution of the request would impair sovereignty, security, public order and essential public interest of India or foreign country.

b) the request for assistance has been made for the purpose of investigating and prosecuting a person on account of that person's sex, race, religion, nationality, origin or political opinions or that person's position may be prejudiced for any of those reasons.

c) the request is made for conduct or offence which is an offence under military law but not an offence under ordinary criminal law in India or foreign country.

d) the request relates to an offence in respect of which the accused person has been finally acquitted or pardoned.

e) de minimis request is made i.e., the request is trivial or disproportionate in nature.

f) the request seeking restraint, forfeiture or confiscation of proceeds and instrumentalities of crime or seizure of property is in respect of conduct/activity which cannot be made the basis for such restraint, forfeiture, confiscation or seizure in the Contracting States [Part I, I. para 1.14, 1.15 of the MHA Guidelines].

In addition, the execution of request may be postponed if it would interfere with an ongoing criminal investigation, prosecution or proceeding in the Contracting States. Such requests may be executed subject to conditions determined necessary after consultations with the Central Authority of the Requesting Country.

**Criterion 37.4 –**

***Criterion 37.4 (a)*** - The detailed guidelines for MLA issued by MHA do not mention restrictive conditions on exchange of information or provision of assistance on the sole ground that the offence is also considered to involve fiscal matters.

***Criterion 37.4 (b)*** - The detailed guidelines for MLA issued by MHA do not mention restrictive conditions on exchange of information or provision of assistance on the grounds of secrecy or confidentiality requirements on financial institutions or DNFBPs.

***Criterion 37.5 –*** The MHA Guidelines set out the requirements for the request for assistance, and its contents and supporting documents must be kept confidential. In the event that a request cannot be executed without breaching confidentiality, the foreign country is required to be informed. Authorities are required to gain the consent of the requesting country to disclose the contents of the request or to utilise any information or evidence provided by that country for any other purpose as set out in the templates for MLA requests. Confidentiality clauses are also included in the treaties for MLA which India enters into.

***Criterion 37.6 –*** 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. 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. In negotiating a MLAT, India refers to the Indian Standard Draft which explicitly states that assistance be given "without regard to whether the conduct which is the subject of investigation, prosecution or proceedings in the Requesting state would constitute an offence under the domestic laws of the Requested State".

***Criterion 37.7 –*** India takes a conduct or activity-based approach to dual criminality where it is required for coercive actions. When executing MLA requests for asset recovery, the dual criminality requirement is satisfied if the conduct underlying the offence would be considered a crime in both states [Paragraph 1.14(vi) of the MHA Guidelines],This extends to the use of coercive powers for ML, TF and predicate offences ( Part C (ii) of the NIA SOP).

***Criterion 37.8 –*** Powers and investigative techniques that are required under Recommendation 31 or otherwise available to domestic competent authorities are available for use in response to requests for mutual legal assistance, with the deficiencies noted in relation to undercover operations interception of communications and controlled delivery also applicable to the execution of MLA requests. Powers are also established for competent authorities in seizing information and evidence in executing MLA requests [Section 105 (Reciprocal arrangements regarding processes) and 166B (Letter of request from a country or place outside India to a Court or an authority for investigation in India) of the Cr.PC].

Competent authorities are empowered to provide a wide range of assistance in tracing, identifying, attaching, seizing and forfeiture of property, if a request in this regard is received from a country or jurisdiction with which there exists a bilateral or multilateral treaty or on the basis of Assurance of Reciprocity [Sections 105A to 105L) of the Cr.PC; Section 58 and Section 59 of PMLA].

### *Weighting and Conclusion*

India has a framework that enables it to provide a wide range of mutual legal assistance, primarily through the CrPC and PMLA. However, there are minor shortcomings regarding impediments to the use of some investigative techniques domestically in response to requests.

**Recommendation 37 is rated largely compliant.**

## Recommendation 38 – Mutual legal assistance: freezing and confiscation

India was rated largely compliant with the former R.38 in its 2010 MER. Deficiencies in its confiscation regime in relation to property laundered, instrumentalities and criminal proceeds were noted as limiting MLA.

***Criterion 38.1 –*** A procedure is set out in legislation for receiving and executing international request to freeze, seize, or confiscate assets in India [Sections 58, 59, 60(2), 60(2A) and provisions of Chapter III and Chapter V of the PMLA]. If the request is deemed complete and fit to be executed, the Central Authority is empowered to forward these requests to the relevant authority for their action or to promptly inform the requesting country that the request has been refused or postponed [S.58, PMLA; 2.2-2.3, MHA Guidelines]. The minor scope gap on predicate offences, as noted in R.3 and R.4, may impact India's ability to respond to international requests of assets related to those offences.

***Criterion 38.1 (a)*** - Definitions of "property" are consistent with the FATF definition and extend to responding to requests from foreign countries [Section 2(v) of PMLA; Section 105A(c) of Cr.PC].

***Criterion 38.1 (b)*** - Definitions of "proceeds of crime" are consistent with the FATF definition and extend to responding to requests from foreign countries [Section 2(u) of PMLA; Section 105A(c) of Cr.PC].

***Criterion 38.1 (c)*** - The term "property" includes property of any kind, including instrumentalities, used in the commission of an offence under this Act or any of the scheduled offences [Section 2(v) of PMLA].

***Criterion 38.1 (d)*** – The terms "proceeds of crime" and "property", as further explained in the footnoted explanations, extend to instrumentalities which may be indirectly involved, or used in the attempt to commit an offence [Sections 2(u) and (v) of PMLA]. India is authorised to respond to international requests to freeze, seize, or confiscate instrumentalities intended for use in ML, TF or predicate offences.

***Criterion 38.1 (e)*** - Definitions of "property" include property equivalent in value held within the country or abroad [Section 2(u) of PMLA; Section 105A(c) of Cr.PC].

***Criterion 38.2*** – Under Indian law, generally the assets can be confiscated or forfeited only after conclusion of criminal trial and conviction. However, India is empowered to provide assistance on the basis of non-conviction-based confiscation proceedings and related provisional measures, in certain scenarios as outlined below.

If a request is received from a foreign country, where the trial under the law of a contracting State cannot be conducted due to death of the accused or being declared a proclaimed offender or for any other reason, the Special Court can pass appropriate orders regarding confiscation or release of property, as per the provisions regarding property involved in the offence of ML, on receipt of a letter of request [Section 58B of the PMLA]. It is not clear what would constitute "any other reason" in this instance.

***Criterion 38.3 –*** Arrangements for co-ordinating seizure and confiscation actions with other countries are set out in the Cr.PC and PMLA. India has ratified 40 MLATs for the coordination of seizure of confiscation actions with other countries. Procedures are in place for the execution of a Letter of Request from a country or place outside India to a Court or an authority for investigation in India and assistance in relation to orders of attachment or forfeiture of property [Sections 166B and 105C of Cr. PC].

In the context of ML, arrangements are in place for coordinating seizure, freezing and confiscation actions with other countries [Section 60 of the PMLA]. Similarly, mechanisms exist for managing, and when necessary, disposing of, property frozen, seized or confiscated [Cr. PC, PMLA and The Prevention of Money Laundering (Receipt & Management of confiscated properties) Rules 2005].

The Court may appoint the District Magistrate or any other officer nominated by District Magistrate, to perform the functions of an Administrator of properties seized or forfeited including receiving and managing the property in relation to which order has been made, subject to such conditions as may be specified by the Central Government [Sections 105E(1), 105F and 105H of Cr.PC]. The Administrator can also take such measures as the Central Government may direct to dispose of the property which is forfeited.

The Administrator is bound to manage confiscated properties and to take such measures, as the Central Government may direct, to dispose of the property which is vested in the Central Government [Section 10(3) of the PMLA].

The administrator shall arrange for the proper maintenance and custody of confiscated property at the place of attachment where it is impractical to remove a confiscated property from the place of attachment or it involves expenditure out of proportion to the value of confiscated

property [The Prevention of Money Laundering (Receipt & Management of confiscated properties) Rules 2005; sub-section (1) of section 15 of PMLA.]. It further provides that the Administrator shall cause to deposit the confiscated property in the nearest Government Treasury or branch of RBI or SBI or its subsidiaries or any authorised bank if the confiscated property consists of cash, Government or other securities, bullions, jewellery or other valuables. The administrator is also required to maintain registers for movable and immovable properties and to obtain a receipt of movable properties deposits.

***Criterion 38.4 –*** When any property in India is confiscated as a result of execution of a request from a contracting State in accordance with the provisions of this Act, the Central Government may either return such property to the requesting State or compensate that State by disposal of such property on mutually agreed terms [Section 60(7) of the PMLA]. The terms would take into account deduction for reasonable expenses incurred in investigation, prosecution or judicial proceedings leading to the return or disposal of confiscated property.

Provisions are also in place for seizure and attachment in India on the basis of request of Contracting State and in accordance with the Bilateral Treaties/Agreements [Sections 105A to 105L of Cr.PC].

### *Weighting and Conclusion*

The legal framework for MLA relating to freezing and confiscation covers most required elements. Minor deficiencies exist in relation to the scope of certain predicate offences, as discussed in R.3 and R.4, for which a clear legal basis for MLA is not provided, or whether the provisions for providing assistance extend to when the perpetrator is unknown.

**Recommendation 38 is rated largely compliant**

## Recommendation 39 – Extradition

India was rated largely compliant with the former R.39 in its 2010 MER. Deficiencies in the criminalisation of ML were found to potentially limit the possibilities for extradition where dual criminality was required.

**Criterion 39.1 –**

***Criterion 39.1 (a)*** – The extradition of fugitives is done as per the provisions of the Extradition Act, 1962 and as per Extradition Treaty or other Extradition Arrangement or International Conventions signed by India with the country concerned.

ML and TF are extraditable offences [Section 4 and para 4 of the PMLA Schedule; Sections 17, 39(2) and 40 of UAPA; Act, 1962 (Section 2(c) of the Extradition Act 1962].

***Criterion 39.1 (b)*** - A request for extradition has to be made as per the provisions of the Extradition Act, 1962 (either Chapter II or Chapter III) and the Treaty with the Contracting State on the reciprocal basis as defined [Section 2(f); Chapters II and III of the Extradition Act; and Section 59 of PMLA].

The Ministry of External Affairs (MEA) is the Central Authority for the requests of extradition [The Extradition Rules, 2017]. In the MEA, the Consular Passport Visa (CPV) Division is responsible for performs the functions of the Central Authority and processes all outgoing and incoming extradition requests. The Extradition Section within the CPV Division has an established procedure to help ensure timely execution of extradition requests, including prioritisation, and has various registers for tracking purposes [MEA SOP for Incoming and Outgoing Extradition Requests, T- 413/P/2021]

Priority is given to urgent and provisional arrest requests and requests concerning ML TF cases, serious crimes, and financial fraud cases. Provisional arrest requests can be forwarded through INTERPOL channels. There are specified contact points in the MHA, IS-II Division and MEA, CPV Division to help ensure better and timely coordination between the Ministries, LEAs, Indian Missions abroad, and the Legal Attorneys that are handling extradition requests [Part VII of the MHA Guidelines].

***Criterion 39.1 (c)*** - Potential cases and grounds for refusal to extradite set out in law or contained in the relevant extradition treaty [Sections 29 and 31 of the Extradition Act]. These grounds are not considered unduly restrictive. Generally, these grounds are:

i. where a person's extradition is sought for an offence of a political character. However, the Extradition Act, 1962 in general and the extradition treaties, in particular, also list out many offences which shall not be considered as an offence of a political character;

ii. the offence of which a person is accused or convicted for a military offence;

iii. if the person whose extradition is sought has, according to the law of the Requesting Country becomes immune from prosecution or punishment by reason of lapse of time;

iv. the person has been tried and acquitted/pardoned/ undergone punishment with respect to the offence for which his extradition is sought; or

v. if the Requested Country has substantial grounds to believe that the person's extradition is sought for the purpose of prosecuting or punishing the person on account of his/her sex, race, religion, nationality, or political opinions, or that the person's position may be prejudiced for any of those reasons [Paragraph 7.4 of the MHA Guidelines].

**Criterion 39.2 –**

***Criterion 39.2 (a)*** - India does not prevent the extradition of Indian nationals on the sole basis of nationality [Section 26 of the Extradition Act]. In practice, the extradition of nationals is considered on the basis of reciprocity as per the provisions of applicable Extradition Treaty.

***Criterion 39.2 (b)*** - If the extradition is refused on the ground of nationality, in terms of the relevant treaty provision, the case, upon request, will be submitted without delay to the competent authorities for the purpose of prosecution [Sections 34 and 34A of the Extradition Act]. CBI is the designated Nodal Agency for the local prosecution of fugitive offenders.

***Criterion 39.3 –*** Dual criminality is an essential part of the extradition process in India. India applies a conduct-based approach for satisfying dual criminality. In the assessment of dual criminality, it does not matter whether the conduct falls within the same category of offences or describe the conduct by the same terminology provided that the conduct in question is criminalised in both the Requested and the Requesting State [2(a) of the Extradition Act].

***Criterion 39.4 –*** The provisional arrest request can be transmitted to appropriate authorities through INTEPROL channels. India applies simplified extradition mechanism for countries to which Chapter III of the Extradition Act is applicable [Section 15 read with 17 of the Extradition Act]. This mechanism of transmission through INTERPOL is currently applicable in India's extradition treaties with seven countries. Further, the Court adopts simplified extradition where the fugitive criminal consents for his extradition. In such case the Court records the voluntary consent statement of the accused and recommends his extradition.

### *Weighting and Conclusion*

**Recommendation 39 is rated compliant.**

## Recommendation 40 – Other forms of international cooperation

In its 2010 MER, India was rated largely compliant with the former R.40. There were no clear and effective gateways and mechanisms in place for RBI and IRDAI that would allow for prompt and constructive exchange of confidential information with foreign counterparts.

***Criterion 40.1 –*** Generally, the main AML/CFT competent authorities can provide a range of international cooperation for ML and associated predicate offences. LEAs, including CBI, ED and NIA have established networks and channels for international cooperation, primarily through the National Central Bureau – India (NCB-India) for INTERPOL requests. These agencies are also able to use Foreign Police Liaison officer networks, Joint Working Groups (JWGs) and MOUs signed with foreign counterparts to exchange a wide range of information both spontaneously and upon request. FIU-IND is also able to exchange information with a foreign counterpart both spontaneously and upon request. Financial supervisors are also able to do this on the basis of MOUs, although there is no explicit legal basis for all supervisors to exchange this information, as detailed in c.40.12-40.16.

**Criterion 40.2 –**

***Criterion 40.2 (a)*** – India's constitution allows government agencies provide cooperation under international treaties, agreements and conventions entered into. Indian LEAs are empowered to cooperate with counterparts in any foreign country under a reciprocal agreement [Section 56 of the PMLA]. India is signatory to a several Multilateral Treaties and Conventions including the UNCAC and UNTOC, which provide for close cooperation between parties for exchange of information and intelligence on an informal basis, further elucidated in the MHA Guidelines [MHA Guidelines, Paras 1.1-1.3].

Other LEAs, specifically, the DRI and Indian Customs exchange information for facilitating trade on the basis of the enabling provisions in its overarching legislation and are required to apply these provisions to agreements signed with 32 contracting States [Section 151B of the Customs Act, 1962; Notification No. 58/2021-Customs (N.T.) dated 1st July 2021].

India has a wide network of tax treaties viz. Double Taxation Avoidance Agreements (DTAAs), Tax Information Exchange Agreements (TIEAs), Multilateral Convention on Mutual Administrative Assistance in Tax Matters (MAAC) and South Asian Association for Regional Cooperation (SAARC) Limited Multilateral Agreement, providing for exchange of information.

FIU-IND is empowered to negotiate, facilitate and administer MOUs with foreign FIUs [OM No.4/10/2004-ES]. FIU-IND is also able to screen and process requests from foreign FIUs, as well as disseminate information to them, even without a bilateral MOU in place, apply for membership in the Egmont Group (it has been a member since 2007), and facilitate the exchange of information with international enforcement agencies and international bodies including the IMF, World Bank and World Customs Organization [OM No.4/10/2004-ES].

There are some deficiencies in financial supervisors' legal basis for providing this cooperation (see c.40.12-c.40.16 below).

***Criterion 40.2 (b)*** – There are no legal impediments to LEAs and FIU-IND using the most efficient means to cooperate. Similarly, financial supervisors provide international cooperation primarily through multilateral and bilateral MOUs and are not impeded from using the most efficient means.

***Criterion 40.2 (c) –*** LEAs have clear and secure channels for the transmission and execution of requests. CBI has been designated National Central Bureau (NCB) for INTERPOL since 1966. The communication through INTERPOL is done through INTERPOL's secure communication channel. Each State Law Enforcement Agency has appointed Liaison Officers for establishing contact with NCB-India, having dedicated staff for coordinating the information exchange, using secure communication channels through official Government emails and/or Indian Postal Services.

The Overseas Investigation Unit (OIU) located at ED Head Quarters, New Delhi receives the informal requests from their foreign counterparts and processes them using the investigative tools available under the provisions of PMLA for providing assistance in response to a request for information from a foreign counterpart agency. All communications related to execution of these requests are made through secured official e-mails or using other physical modes with enhanced security measures.

FIU IND is able to share information with other Egmont members is exchanged via the Egmont Secure Web (ESW).

See c.40.12-c.40.16 for financial supervisors' processes for international cooperation.

***Criterion 40.2 (d)*** – LEAs have clear processes for the prioritisation and timely execution of requests. Communication through INTERPOL channel is governed by Rules on Processing of data of INTERPOL. All the important requests are prioritised through chain of command. The system is manned on a 24/7 basis.

The OIU monitors the progress of the execution of the requests and ensures that responses are provided promptly to foreign authorities/agencies in case of urgency. Each request is treated as a separate case and is given a separate file number for monitoring purposes, including through domestically coordinated responses.

FIU-IND adheres to the Egmont principles on exchange of information for prioritisation and execution.

See c.40.12-c.40.16 for financial supervisors' processes for international cooperation.

***Criterion 40.2 (e) –***

LEAs have processes for safeguarding the information received and exchanged. -India has systems put in place for restrictive access to the system to maintain due confidentiality. In particular, OIU ensures confidentiality of requests and information exchanged through appropriate safeguards and procedures.

The tax treaties provide that any information received shall be treated as secret in the same manner as information obtained under India's domestic laws. The Information Security Policy of CBDT addresses internal and external information security risks and protects the availability, confidentiality, and integrity of information obtained under the tax treaties.

Specific articles in Customs Mutual Assistance Agreements (CMAA) maintain the confidentiality of information shared between the partner countries.

FIU-IND has internal procedures for safeguarding the information received from foreign counterparts and how such information is to be handled.

Financial supervisors have processes for safeguarding the information received and exchanged as set out in their various bilateral and multilateral MOUs. See. c.40.12-c.40.16 for details.

***Criterion 40.3 –*** The Central Government may enter into an agreement with the Government of any country outside India for— (a) enforcing the provisions of the PMLA; or (b) exchange of

information for the prevention or investigation of any offence under the PMLA or under the corresponding law in force in that country [Section 56 of PMLA].

The Central Government may, by notification, subject such agreements to conditions, exceptions and qualifications as are specified in the said notification [Section 56(2) of PMLA]. Therefore, exchange of information including intelligence can be undertaken by the Directorate under a specified arrangement entered into on the basis of this section.

The Central Government may also enter into international agreements as per the constitution but there are no express provisions regarding the time frame to negotiate and sign such agreements. It is through this mechanism that the NIA is able to share information related to TF.

India has negotiated and signed 35 Customs Mutual Administrative Agreements (CMAAs) involving more than 60 countries for investigative assistance. DRI honours information requests received from non-counterparts under the Customs Mutual Administrative Agreements (CMAAs). This is done under the International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offences (Nairobi Convention).

India has a wide network of tax treaties viz. Double Taxation Avoidance Agreements (DTAAs), Tax Information Exchange Agreements (TIEAs), Multilateral Convention on Mutual Administrative Assistance in Tax Matters (MAAC) and South Asian Association for Regional Cooperation (SAARC) Limited Multilateral Agreement, providing for exchange of information.

FIU-IND is empowered to sign MOUs with foreign FIUs in order to enhance co-operation and has negotiated and entered into bilateral MOUs with 49 FIUs as of November 2023. FIU-IND is also able to share information with foreign counterparts on the basis of reciprocity.

Financial supervisors have processes for safeguarding the information received and exchanged as set out in their various bilateral and multilateral MOUs. There are some deficiencies in RBI's legal basis for providing this cooperation (see c.40.12-c.40.16 below).

***Criterion 40.4 –*** AML/CFT competent authorities are able to provide feedback on the use and usefulness of information obtained coordinated through monthly, quarterly and biannual reviews [ MHA Guidelines, Paras 2.5-2.7]. LEAs have various mechanisms for this. CBI provides feedback upon request and on a case-by-case basis and DRI/Indian Customs are also able to provide feedback as set out in the CMAAs. ED has a structured feedback process as set out in Technical Circular No. 11/2023. The NIA also able to provide feedback upon request through the same channel by which information was requested.

AML/CFT supervisors are able to provide feedback upon request as set out in the various MOUs entered into. For example, SEBI has provided feedback on seven requests from one authority in the last three years.

**Criterion 40.5 –**

***Criterion 40.5 (a)*** –India does not place unreasonable or unduly restrictive conditions on the exchange of information and assistance is not refused if the request involves fiscal matters [Para 1.14 of the Guidelines on Mutual Legal Assistance in Criminal Matters No.25016/52/2019-LC]. Other forms of cooperation are guided by the bilateral, regional and international cooperation networks and arrangements to which India is a party and unreasonable or unduly restrictive conditions are applied.

***Criterion 40.5 (b)*** - Execution of requests should not be refused solely on the ground of bank secrecy according to the Guidelines issued to facilitate MLA [Para 1.16 of the Guidelines on Mutual Legal Assistance in Criminal Matters No.25016/52/2019-LC]. Other forms of cooperation are guided by the bilateral, regional and international cooperation networks and arrangements to which India is a party and requests are not refused solely due to bank secrecy.

***Criterion 40.5 (c)*** - The execution of a request may be postponed if it would interfere with an ongoing criminal investigation, prosecution or proceeding in the Contracting States. Such a request may be executed subject to conditions determined necessary after consultation with the Central Authority of the Requesting Country [Para 1.15 of the Guidelines on Mutual Legal Assistance in Criminal Matters No.25016/52/2019-LC]. Other forms of requests outside of MLA are also informed by the above provisions as well as the bilateral, regional and international cooperation networks and arrangements to which India is a party.

***Criterion 40.5 (d)*** – There are no provisions in Indian legislation which prohibit or restrict the exchange of information on the grounds that the counterpart authority is of a different nature or status.

***Criterion 40.6*** –

LEAs have controls to safeguard the information received and ensure it is used only for its intended purposes. CBI and CBDT have internal policies and procedures regarding safeguards and controls for information shared. The ED relies on the procedural requirements as established in the networks it belongs to ensure the information exchanged is used for the purpose requested. India's tax treaties contain provisions on confidentiality and use of information exchanged. issued by The CBDT has issued comprehensive guidelines to the field authorities in relation to handling of information exchanged by competent authorities for tax purposes [Chapter-III Para 3.8 (Guidelines for utilisation of information and maintaining confidentiality) and Chapter-VII (Confidentiality) of the Manual on Exchange of Information 2015]. This seeks to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorization has been given by the requested competent authority.

FIU-IND is a member of the Egmont Group and therefore must abide by the Egmont principles of information exchange. In addition to attaching a detailed disclaimer to any information shared with Indian agencies, whenever information is sought from a counterpart FIU on behalf of law enforcement agencies, necessary sanitisation e.g., the source of foreign intelligence is not divulged, and is done before sharing the material.

Financial supervisors have processes for safeguarding the information received and ensuring it is used only for its intended purpose as set out in their various bilateral and multilateral MOUs (see c.40.12-c.40.16 below).

Further, overarching Indian legislation establishes controls and safeguards to protect information, including making it an offence for the wrongful communication of information in case it affects friendly relations with foreign states [S.5, Official Secrets Act, 1923]. India also has freedom of information legislation in force, with specific exemptions for intelligence and security agencies, and allowing for the Central Government to block access by the public to certain sensitive information that pertains to the integrity, defence, security of the state or friendly relations with foreign states [S.24, Right to Information Act, 2005; Information Technology Act, 2000; Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009].

***Criterion 40.7 –*** LEAs, including ED, NIA, CBI, CBDT, and FIU-IND have internal procedures and guidelines regarding confidentiality requirements. These include strict physical and electronic security of information, and the use of official and secured channels to protect information when being shared to relevant officials, in the same manner as information received from domestic sources. In addition, confidentiality clauses are included in the MOUs and MMOUs entered into by competent authorities.

Financial supervisors have internal procedures and guidelines regarding confidentiality requirements associated with the commercially and personally sensitive information they have access to. In addition, confidentiality clauses are included in the MOUs and MMOUs entered into by financial supervisors.

***Criterion 40.8 –*** LEAs are empowered to conduct inquiries on behalf of foreign counterparts. For ED in particular, the term "inquiry" is defined as a step necessary for tracing and identifying property as part of execution of a letter of request "received from a court or an authority in a contracting State requesting attachment, **seizure**, freezing or confiscation of the property in India, derived or obtained, directly or indirectly, by any person from the commission of an offence under a corresponding law committed in that contracting State" [Sections 60 (3)(4), PMLA]. Assistance is provided upon receipt of a letter of request to the Central Government which may then forward this request to the Special Court or any other authority for execution [S. 58,PMLA].

Other LEAs are able to use legal provisions enable Indian Authorities to seize/attach of property while conducting an inquiry on behalf of foreign authorities [Sections 105D -105K, Cr.PC]. The term "inquiry" in this context means every inquiry, other than a trial, conducted under this Code by a Magistrate or Court [Article 2(g), Cr.PC].

Upon receipt of a letter of request from a Court or an authority in a country or place outside India competent to issue such a letter, the Central Government may send the letter to any police officer for investigation, who is to investigate the offence in the same manner, as if the offence had been committed within India [S.166B(1)(ii), Cr.PC].

FIU-IND is able to make inquiries on behalf of foreign FIUs through the Egmont Secure Web.

Please refer to Criterion 40.15 for the review of inquiries conducted by financial supervisors.

***Criterion 40.9 –*** FIU-IND has an adequate legal basis for providing co-operation on ML, associated predicate offences and TF [para 3 of OM No. 4/10/2004].

***Criterion 40.10 –*** FIU-IND provides feedback to foreign counterparts using uniform templates upon request on the use of the information provided according to the Principles of Information Exchange of the Egmont Group. In 2021 and 2022, such feedback was provided to five countries. FIU-IND provides feedback to foreign counterparts based on inputs from the concerned LEAs with whom the intelligence, as received from foreign FIUs, was shared. Feedback has been shared in respect of individual request-based intelligence and spontaneous disclosures.

**Criterion 40.11 –**

***Criterion 40.11 (a)*** – FIU-IND is able to share all information domestically available, including STRs and other information from the reporting entities [Sections 12, 13 and 50, PMLA]. The FIU is empowered to disseminate information with foreign FIUs, although without explicit reference to the sharing of operational or strategic analysis although these have been shared with foreign counterparts (OM No. 4/10/2004).

***Criterion 40.11 (b)*** - FIU-IND is able to obtain domestically other information which is necessary to perform its functions, including from competent authorities, and is empowered to share this information with foreign FIUs [Section 66 of PMLA; OM No. 4/10/2004]. See also Criterion 40.9 above.

***Criterion 40.12 –***

RBI (Banks and other FIs): There is no explicit legislation allowing or not allowing RBI to cooperate with foreign counterparts. However, RBI has entered into Memoranda of Understanding (MoUs), Exchanges of Letters on supervisory co-operation (EoLs) and

Statements of co-operation (SoCs) with overseas supervisors for supervisory cooperation on the strength of the Department of Financial Services [MOF letter dated 27th February 2012].

SEBI (Securities): SEBI is empowered to share information with foreign authorities having functions similar to those of SEBI in matters relating to the prevention or detection of violations in respect of securities laws, and to enter into an arrangement or agreement or understanding with such authorities [Section 11(2)(ib) of the SEBI Act, 1992]. Accordingly, SEBI has become a signatory to the International Organisation of Securities Commission (IOSCO) MMoU in April 22, 2003, and has signed bilateral MoUs with various foreign authorities which enable the signatories to consult periodically with each other about matters of common concern and for resolving any issues.

IRDAI (Insurance): IRDAI is empowered to share information with foreign counterparts, with MoUs and MMoUs setting out the manner in which information can be shared [Sections 3 and 4 of the IRDAI (Sharing of Confidential Information Concerning Domestic or Foreign Entity) Regulations, 2012.

IRDAI is a signatory to the MMOU of IAIS which provides formal basis for cooperation and information exchange. There are 81 signatories to this MMoU as on January 2023. Matters pertaining to AML/CFT are specifically mentioned in the objective and scope of the MMOU. IRDAI has also entered into MoU with Federal Insurance Office (FIO) United States Dept. of the Treasury and Insurance Authority of UAE for cooperation, coordination and exchange of information.

PFRDA: There is no legislation allowing or not allowing PFRDA to cooperate with foreign counterparts. The relevant FIs currently under supervision do not engage with foreign entities due to the nature of the products and services offered. However, PFRDA is a member of the International Organization of Pension Supervisors (IOPS).

IFSCA: IFSCA is empowered to enter into MOUs in order to perform its role as a regulator and has entered into six MOUs with foreign counterparts [Section 13(1) of the IFSCA Act, 2019]. This does not explicitly include the sharing of information in its capacity as AML/CFT supervisor, but is not restricted from doing so.

***Criterion 40.13 –***

It is unclear that the following provisions provide for the possibility of all financial supervisors to exchange information held by financial institutions with foreign counterparts.

RBI (Banks and other FIs): As per c.40.12 above, there is no explicit legal basis for international cooperation. However, based on Basel Core Principles (BCP) on 'Home- Host relationships,' RBI has established formal arrangements in MoUs, EoLs and SoCs with overseas supervisory authorities for information sharing and supervisory co-operation with respect to cross border banking organisations.

RBI has executed 43 MoUs, two EoLs and one SoC with overseas supervisors and regulators as on date, with some containing explicit provisions regarding the type of information that can be exchanged.

SEBI (Securities): SEBI has information gathering powers under the SEBI Act to obtain the necessary information to assist foreign securities regulators. SEBI has signed Bilateral MoUs with 26 securities regulators for enhancing cooperation and exchange of information for regulatory and enforcement purposes.

IRDAI (Insurance): IRDAI is able to exchange with foreign counterparts information domestically available to them. Regulations set out the basis for, sharing of information available in public domain and, in case of information not available in public domain, consideration of

reasons for request made, nature of information sought, maintenance of confidentiality of information and reciprocity of request [Regulation 4(i) of IRDAI (Sharing of Confidential Information Concerning Domestic or Foreign Entity) Regulations, 2012].

PFRDA: As per c.40.12, PFRDA does not have mechanisms to exchange information and has not entered into any MOUs with foreign counterparts as supervised FIs do not engage with the operations of foreign entities.

IFSCA: IFSCA has entered into six MOUs for the sharing of information, although information held by FIs is not explicitly included or excluded.

***Criterion 40.14 –*** RBI (Banks and other FIs): As per c.40.12 above, there is no explicit legal basis for international cooperation. However, the MoUs EoLs and SoCs provides for sharing of information on the supervised entities (including KYC/ML/TF related information), cooperation between supervisors during on site examination, coordinated efforts during times of crisis, frequent meetings between the supervisors, and preserving the confidentiality of information shared etc. These arrangements may include the sharing of prudential information, and AML/CFT information such as CDD information, customer files, samples of accounts and transaction information, where relevant to the supervisory requirements and permissible by law.

The RBI has established Supervisory Colleges for six large Indian banks, which are internationally active. The College meets once in two years in India to discuss supervisory issues, including KYC AML issues, Trade based money laundering threats, Screening systems, etc. These Colleges met in virtual format in 2021 with an average of approximately nine supervisors in attendance at each meeting. The meetings in 2023 were held in physical mode in which twenty supervisors from ten overseas supervisory jurisdictions participated.

SEBI (Securities): SEBI is appropriately empowered and, in a position, to exchange the information in relation to the prevention or detection of violations of securities laws with foreign counterparts and to enter into the necessary arrangements [Section 11 of the SEBI Act]. SEBI is a member of the IOSCO Board and one of 124 signatories to the IOSCO MMoU. This MMoU is broad and is in accordance with best practices.

SEBI extends the widest possible co-operation with foreign counterparts for exchange of information and provides assistance to its foreign counterparts whenever they seek to obtain beneficial ownership related information for their enforcement functions. For example, foreign securities regulators have requested SEBI for various documents like KYC documents/ bank records/incorporation documents/share certificates, etc. in relation to their investigations into securities laws violations. In addition to the above, necessary details are provided to foreign securities regulator regarding beneficial ownership details for assessment of applicants.

IRDAI (Insurance): IRDAI is able to exchange with foreign counterparts the information domestically available to them through MoUs, MMoUs [Regulation 3 and 4 IRDA (Sharing of Confidential Information Concerning Domestic or Foreign Entity) Regulations, 2012] Further, IRDAI as part of 'Fit & Proper' tests seek due diligence reports from foreign counterparts, wherever applicable.

PFRDA: PFRDA does not engage in information sharing with foreign counterparts.

IFSCA: IFSCA is able to share information with foreign counterparts pursuant to the IOSCO MMoU (Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information). This MMoU includes a broad scope of information exchange that can be expanded to other laws and regulations within the competencies of the cooperating parties. IFSCA became a signatory to the IAIS MMoU in November 2023 to enhance its capacity to exchange information.

***Criterion 40.15 –*** RBI (Banks and other FIs): As per c.40.12 above, there is no explicit legal basis for international cooperation. However, there are provisions for onsite examinations in the MoUs which enable competent authorities to conduct inquiries on behalf of foreign counterparts, and to authorise or facilitate foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision .

SEBI (Securities): Assistance is provided to foreign securities regulators under the aegis of IOSCO MMoUs and bilateral MoUs on the matters pertaining to securities market, as per the applicable laws.

While there is no specific power to conduct investigation on behalf of other foreign agencies, however, SEBI has been assisting foreign regulators under the aegis of MMoUs and bilateral MoUs. The scope of assistance 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.

IRDAI (Insurance): The MoU entered by IRDAI has provision to provide investigative assistance with respect to each authority's oversight and other lawful responsibilities.

PFRDA: PFRDA does not engage in information sharing with foreign counterparts.

IFSCA: As per c.40.13 and c40.14 above, IFSCA has entered into six bilateral MoUs and the IOSCO and IAIA MMoUs which include conducting inquiries on behalf of foreign counterparts and the recovery of related costs.

***Criterion 40.16 –*** Financial supervisors in India ensure that they have the prior authorisation of the requested financial supervisor for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes.

RBI (Banks and other FIs): As per c.40.12 above, there is no explicit legal basis for international cooperation. However, the provisions in the MoUs established with overseas central banks requires the signing authorities to use any confidential information shared only for their respective lawful supervisory purposes. All such information is treated as confidential and prior written consent of the other authority is obtained for disclosure.

SEBI (Securities): The information provided by a Requested Authority to a Requesting Authority pursuant to a request made under the IOSCO MMOU is subject to confidentiality and permissible use clauses under the IOSCO MMOU S.10 ISOCO MMoU].

IRDAI (Insurance): The requirements are covered in the provisions of para 3(vii) and 3(viii) of IRDA (Sharing of Confidential Information Concerning Domestic or Foreign Entity) Regulations, 2012. Similar provisions are also set out in article 5 and Annex B of the IAIS MMOU, to which IRDAI has been a signatory since May 2013.

PFRDA: PFRDA does not engage in information sharing with foreign counterparts.

IFSCA: IFSCA is required to obtain the consent of the requested financial supervisor for the dissemination of information exchanged [S.14, IFSC Regulations 2023]. Specific provisions on confidentiality and use of information are contained in the MOUs, including the IOSCO and IAIS MMoUs.

***Criterion 40.17 –*** INTERPOL channels and Foreign Police Liaison officer networks are used for extensive sharing of information and intelligence on crime including money laundering, terror financing and on proceeds of crime, with CBI as the central point on ML and predicate matters. LEAs are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering or associated predicate

offences. This includes the identification and tracing of the proceeds and instrumentalities of crime. LEAs are empowered to ensure that domestically available information is able to be shared directly for international cooperation and assistance where ML is involved [Sections 52 and 56, PMLA].

Customs officials also have the ability to exchange information pertaining to declarations/disclosures [Section 151(b) of the Customs Act].

The NIA is able to share domestically available information on TF with foreign counterparts through Foreign Police Liaison officer networks and MoUs with foreign counterparts. The NIA has currently entered into an MoU with the Royal Canadian Mounted Police.

***Criterion 40.18 –*** As per c.40.17 above, LEAs are empowered to exchange domestically available information with foreign counterparts for intelligence or investigative purposes. This is coordinated through the NCB India (CBI) with processes set out in SOPs and the MHA Guidelines.

***Criterion 40.19 –*** Law enforcement authorities, such as CBI, ED, DRI and Indian Customs, are able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations. The "offence of cross border implication" is defined in such a manner that ML investigation can be initiated in India if an ML offence has taken place in a foreign country and proceeds of crime have been transferred to India [Section 2(1)(ra), PMLA].

Para 5.10 of the aforementioned MHA Guidelines provide the mechanism to establish joint investigative teams in India. The specific arrangements entered into for the purposes of a joint investigative team are to be mutually agreed between the contracting state.

To date, these joint investigative teams have consisted largely of foreign law enforcement officials witnessing the interviewing of witnesses located in India.

Customs officials are also able to establish joint investigative teams under relevant clauses in the CMAAs with various countries and organisations.

In addition to above, India is also signatory to UNCAC and UNTOC, both of which provide for Joint Investigations [Article 49 of UNCAC and Article 19 of UNTOC].

***Criterion 40.20 –*** The competent authorities in India are able to exchange information indirectly with non-counterparts as there is no express provision in legislation to prevent competent authorities from indirectly sharing information with non-counterparts. These requests may be routed through CBI utilising INTERPOL channels to share with foreign LEAs, or though FIU-IND to utilise the Egmont Group network and then forwarded for execution to relevant non-counterpart competent authorities. For this purpose, an MoU was entered into between FIU-IND and the Central Board of Direct Taxes (CBDT) in which it has been provided that if CBDT requires information from a foreign FIU, a request will be made to FIU-IND in Egmont prescribed proforma in electronic format and CBDT shall abide by the conditions that may be imposed by the foreign FIU on the use of information provided by the foreign FIU [to para 6.4.3 of the Manual 2015 for Information Exchange with foreign tax authorities, on 20th September, 2013].

Similarly, the MoU between ED and FIU-IND provides an overview of how ED may seek and provide information to foreign FIUs.

RBI is able to share information with non-counterparts through the provisions in MOUs related to the sharing of information with third parties.

SEBI: Under the IOSCO MMOU, non-counterparts may seek information from SEBI via their domestic securities market regulator, which would be treated by SEBI as a request from a counterpart and responded to accordingly.

IRDAI is able to share information with non-counterparts. Where it becomes necessary for a Requesting Authority to share Confidential Information provided under this MMoU with other local, regional, state, federal or international law enforcement or regulatory officials who have authority over the Regulated Entity, the Requesting Authority shall: a. notify the Requested Authority promptly; b. obtain prior consent; and c. prior to passing on the information, ensure that each recipient agrees to maintain the confidential status of the information provided and has the legal authority to do so" [para 9 Art. 5 of the IAIS MMOU].

PFRDA: PFRDA does not engage in information sharing with foreign counterparts or non-counterparts.

IFSCA is able to share information with non-counterparts through provisions in MOUs regarding the sharing of information with prior consent.

The ability for other supervisors to exchange information indirectly with non-counterparts has not been provided.

### *Weighting and Conclusion*

There are minor shortcomings in India's ability the provide other forms of international cooperation. These relate to the timeliness of establishing MoUs, as well as the legal basis for some financial supervisors (RBI and PFRDA) to enter into these arrangements which has been weighted according to the risk and materiality of these sectors. Minor deficiencies also remain in relation to supervisors' ability to share information held by FIs.

**Recommendation 40 is rated largely compliant**.

# SUMMARY OF TECHNICAL COMPLIANCE - KEY DEFICIENCIES

## Compliance with FATF Recommendations

| Recommendations | Rating | Factor(s) underlying the rating |
|---|---|---|
| 1. Assessing risks & applying a risk-based approach | LC | Not demonstrated that the allocation of resources such as staffing across the other authorities dealing with financial investigations is being informed by the risks identified.<br>Not fully considered how the threats correspond with the exemption applied in the real estate sector.<br>Not been demonstrated that regulators AML/CFT supervision is being conducted periodically based on ML/TF risk.<br>No specific authority has been given powers and responsibilities for AML/CFT supervision for chartered accountants, notaries, lawyers and company secretaries. |
| 2. National cooperation and coordination | C | Nil |
| 3. Money laundering offences | LC | India's list approach does not encompass the full range of FATF's designated categories of offences. For smuggling offences the minimum threshold is very high, and for human trafficking and migrant smuggling not all conduct is covered. |
| 4. Confiscation and provisional measures | LC | Scope gap in the coverage of predicate offences (See R.3)<br>Lack of explicit processes for the management of incorporeal property or enterprises |
| 5. Terrorist financing offence | LC | Legislation does not clearly indicate what criminal, civil or administrative liability and sanctions apply to legal persons and thus it is not possible to assess whether sanctions are proportionate and dissuasive. |
| 6. Targeted financial sanctions related to terrorism & TF | LC | Lack of clarity in the language of the OM regarding the implementation of TFA without delay.<br>There are no provisions which explicitly provide liability for failure to comply with TFS obligations by natural and legal persons other than FIs and DNFBPs outside the TF sanctions under the UAPA.<br>There is no clear guidance on TFS obligations for natural and legal persons other than reporting entities.<br>There is no explicit prevention of prosecution or legal proceedings of other persons who in good faith take action in relation to assets when implementing the obligations under the UAPA, except for government officers. |
| 7. Targeted financial sanctions related to proliferation | LC | There is no explicit prevention of prosecution or legal proceedings of other persons who in good faith take action in relation to assets when implementing the obligations under the UAPA, except for government officers.<br>There are no explicit measures through laws and enforceable means requiring DNFBPs to be monitored to ensure compliance with PF-TFS obligations. |
| 8. Non-profit organisations | PC | Measures to address TF risks identified are not specifically targeted at the identified NPO sub-sector that may be abused for TF and thus, it has not been demonstrated that authorities have adapted their action to address risks identified.<br>It has not been demonstrated that outreach and educational programmes extend to the donor community.<br>Authorities do not work with NPOs to develop and refine best practices to address TF risk and vulnerabilities to protect them from TF abuse.<br>It has not been demonstrated that ITD is supervising or monitoring NPOs in a risk-based manner, targeted at these NPOs at risk of TF abuse.<br>It has not been demonstrated that the manner and frequency of the regular monitoring conducted, particularly by ITD, is linked to the risk of TF abuse, or targets NPOs most vulnerable to TF abuse. |
| 9. Financial institution secrecy laws | C | Nil |

| Recommendations | Rating | Factor(s) underlying the rating |
|---|---|---|
| 10. Customer due diligence | LC | There are exceptions to the requirement to verify the customer identity using reliable and independent identification data.<br>It is unclear whether the definition of beneficial owner includes a natural person who exercises ultimate effective control over a legal arrangement.<br>There is an ambiguity in the requirement for insurers to carry out necessary CDD of the policyholders/beneficiaries/legal heirs/assignees before making the pay-outs.<br>There are exceptions to the requirement to conduct CDD as soon as reasonably practicable after the establishment of the business relationship. |
| 11. Record keeping | C | Nil |
| 12. Politically exposed persons | PC | There is some ambiguity in the requirement for some FIs to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as foreign PEPs.<br>For all FI sectors except the IFSC, there are no requirements dealing with domestic PEPs or persons who or have been entrusted with a prominent function by an international organisation. |
| 13. Correspondent banking | C | Nil |
| 14. Money or value transfer services | LC | There are no specific requirements for MVTS providers to include their agents in their AML/CFT programmes. |
| 15. New technologies | LC | India conducted SRA, identifying and assessing the ML and TF risks from VAs and VASPs, but it is somewhat outdated and limited in scope.<br>There are requirements to prevent criminals from owning or controlling or hold a management function in a VASP do not provide for checks to identify criminal associates and to expressly prevent criminals or their associates from being a beneficial owner of a VASP.<br>India has not yet established channels for international cooperation with other VASP supervisors. |
| 16. Wire transfers | C | Nil |
| 17. Reliance on third parties | LC | While FIs are required to satisfy themselves that the third party is not based in a country or jurisdiction assessed as high risk, this is not equivalent to the standard, which requires the FI to have regard to information available on the level of country risk (which is broader than just high risk) when determining in which countries the third party can be based. |
| 18. Internal controls and foreign branches and subsidiaries | LC | There are no specific requirements for the provision, at group-wide level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information in respect of FIs in the banking/ MVTS sector (except in relation to the IFSC). |
| 19. Higher-risk countries | LC | The regulations for the securities, pension and the IFSC fall short of a requirement to be able to apply countermeasures proportionate to risks, as required under c.19.2 |
| 20. Reporting of suspicious transaction | LC | There is some ambiguity on whether the list of suspicious transactions is exhaustive or exemplificative, but guidance has clarified that reporting requirements should be interpret broadly and in line with the standard. |
| 21. Tipping-off and confidentiality | C | Nil. |
| 22. DNFBPs: Customer due diligence | LC | Accountants, lawyers and TCSPs are not considered REs when they are only involved the preparatory work and that impacts all criteria.<br>Deficiencies identified in R.10 and R.12, apply equally to DNFBPs.<br>For lawyers, accountants and TCSPs, there are no obligations for undertaking risk assessments prior to the launch or use of such products, practices and technologies. |
| 23. DNFBPs: Other measures | LC | Deficiencies identified in R.18, R.19 and R.20 apply equally to DNFBPs.<br>Accountants, lawyers and TCSPs are not considered REs when they are only involved the preparatory work, which impacts all relevant criteria. |
| 24. Transparency and beneficial ownership of legal persons | LC | It is not ensured that all records will be kept for at least five years after dissolution of a legal person, although basic and SBO information is also filed with the Registrar.<br>Overall, sanctions appear to be proportionate and dissuasive, although monetary sanctions might not be sufficiently dissuasive for larger businesses.<br>It is unclear if the quality of basic and BO information received by India is sufficiently monitored. |
| 25. Transparency and beneficial ownership of legal arrangements | LC | India has some minor shortcomings in its framework relating to the transparency and beneficial ownership of trusts administered by non-professional trustees and HUFs. Access to adequate, accurate and current information on the identity of the settlor, the trustees, the protector and the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust may not always be ensured (c.25.1 and c.25.2).<br>Sanctions to ensure access to information are not always proportional. |

| Recommendations | Rating | Factor(s) underlying the rating |
|---|---|---|
| 26. Regulation and supervision of financial institutions | LC | There are gaps for market entry in relation to certain (less material) FIs. The fit and proper requirements sometimes do not extend to beneficial owners or are insufficient to identify criminal associations.<br>Whilst supervision is carried out across FI sectors, the application AML/CFT supervision considering ML/TF risks is not clear for all sectors. |
| 27. Powers of supervisors | C | Nil |
| 28. Regulation and supervision of DNFBPs | PC | Some DNFBP sectors are not yet subject to systems of compliance with AML/CFT requirements.<br>Measures in place to prevent criminals or their associates from being professionally accredited, or holding a significant or controlling interest, or holding a management function in a DNFBP differ in intensity between sectors and are not sufficient, in particular for the DPMS and TCSP sectors.<br>Supervisors are in the process of developing risk-based supervision systems for compliance monitoring.<br>There are shortcomings in the enforcement provisions particularly on some of the high-risk sectors. |
| 29. Financial intelligence units | C | Nil |
| 30. Responsibilities of law enforcement and investigative authorities | LC | Responsibly for expeditiously identify, trace, and initiate the freezing and seizing of property (that is, or may become, subject to confiscation) has not been clearly assigned. |
| 31. Powers of law enforcement and investigative authorities | LC | There are no specific provisions for the conduct of undercover operations of intercepting communications. |
| 32. Cash couriers | LC | Records of disclosures are not retained by Customs officials and are not made available to the FIU or for international cooperation purposes<br>No explicit requirement to notify FIU-IND of suspicious cross-border transportation incidents |
| 33. Statistics | C | Nil |
| 34. Guidance and feedback | LC | Guidance and feedback mechanisms are not available for lawyers. |
| 35. Sanctions | LC | There is no specific penalty available for breaches of TFS obligations for natural and legal persons.<br>Financial sanctions under the PMLA may not be dissuasive level, depending on the type of infraction or size of the institution. |
| 36. International instruments | C | Nil. |
| 37. Mutual legal assistance | LC | Deficiencies in application of undercover operations, interception of communications and controlled delivery techniques to execute MLA requests |
| 38. Mutual legal assistance: freezing and confiscation | LC | Minor scope gap in the coverage of predicate offences (see R.3 and 4)<br>Unclear if confiscation extends to when a perpetrator is unknown |
| 39. Extradition | C | Nil |
| 40. Other forms of international cooperation | LC | No express provisions to enters into agreements in a timely manner<br>No legal provision allowing RBI or PFRDA to enter into arrangements to exchange information with foreign counterparts<br>Not all financial supervisors legally empowered to exchange information held by Fis with foreign counterparts |

# Glossary of Acronyms[213]

| | DEFINITION |
|---|---|
| ATM | Automated Teller Machine |
| BO | Beneficial Owner |
| BR Act | Banking Regulation Act |
| CA | Companies Act |
| CBDT | Central Board of Direct Taxes |
| CBI | Central Bureau of Investigation |
| CBIC | Central Board of Indirect Taxes |
| CDF | Currency declaration form |
| CEIB | Central Economic Intelligence Bureau |
| CERT-IN | Computer Emergency Response Team, Ministry of Electronics and Information Technology |
| CKYCR | Central KYC Registry |
| CMAA | Customs Mutual Assistance Agreement |
| CPC | The Code of Criminal Procedure |
| CPF | Counter Proliferation Finance |
| CPVD | Consular Passport Visa Division |
| CRA | Central Recordkeeping Agency |
| CTR | Cash Transaction Report |
| CTCR | Counter Terrorism and Counter Radicalisation Division |
| DD | Due diligence |
| DGFT | Directorate General of Foreign Trade, Ministry of Commerce |
| DNFBP | Designated non-financial businesses and professions |
| DOR | Department of Revenue, Ministry of Finance |
| DOR WMD | Department of Revenue Order concerning prohibition of activities related to weapons of mass destruction |
| DPMS | Dealers in Precious Metals and Stones |
| DRI | Directorate of Revenue Intelligence |
| D&ISA | Disarmament and International Security Affairs, Ministry of External Affairs |
| ED | Enforcement Directorate |
| EDD | Enhanced due diligence |
| EIC | Economic Intelligence Council |
| EoL | Exchangers of letters on supervisory cooperation |
| FCRA | Foreign Contribution Regulation Act |
| FEMA | Foreign Exchange Management Act |
| FEOA | Fugitive Economic Offenders Act |
| FFMC | Fully-fledged money changer |
| FI | Financial Institution |
| FINnet | Financial Intelligence Network (IT platform used by the FIU of India) |
| FINex | LEA module in FINnet |
| FIU-IND | Financial Intelligence Unit of India |
| FPIs | Foreign Portfolio Investors |
| FSAP | Financial Sector Assessment Programme |
| FUR | Follow-up report |
| GST | Goods and Services Tax |

[213] Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

| | DEFINITION |
|---|---|
| HUF | Hindu Undivided Family |
| IAIS | International Association of Insurance Supervisors |
| IAs | Intelligence Agencies |
| IB | Intelligence Bureau |
| IFSC | International Financial Services Centre |
| IFSCA | International Financial Services Centres Authority |
| IMCC | Inter-ministerial Co-ordination Committee |
| i-MoT | Module on Terrorism (online application) |
| IOPS | International Organisation of Pension Supervisors |
| IOSCO | International Organisation of Securities Commission |
| IPC | Indian Penal Code |
| IPCC | INTERPOL Police Cooperation Centre |
| IRDAI | Insurance Development and Regulatory Authority of India |
| I4C | Indian Cybercrime Coordination Centre |
| JWG | Joint Working Group |
| KYC | Know your customer |
| LAB | Local area bank |
| LEA | Law Enforcement Authority |
| LLP | Limited Liability Partnership |
| LLPA | Limited Liability Partnership Act |
| MAAC | Mutual Administrative Assistance in Tax Matters |
| MAC | Multi-agency Centre |
| MCA | Ministry of Corporate Affairs |
| MEA | Ministry of External Affairs |
| MER | Mutual Evaluation Report |
| MHA | Ministry of Home Affairs |
| ML | Money laundering |
| MLA | Mutual Legal Assistance |
| MLAT | Mutual legal assistance treaty |
| MMOU | Multilateral Memorandum of Understanding |
| MOF | Ministry of Finance |
| MOU | Memorandum of Understanding |
| MPR | Monthly progress report |
| MTSS | Money transfer service scheme |
| MVTS | Money or value transfer services |
| NABARD | National Bank for Agriculture and Rural Development |
| NBFC | Non-banking financial companies |
| NDPSA | Narcotics Drugs and Psychotropic Substances Act |
| NCB | Narcotics Control Bureau |
| NIA | National Investigation Agency |
| NRA | National Risk Assessment |
| OAR | Operational Analysis Report |
| OIU | Overseas Investigation Unit |
| OM | Office Memorandum |
| PAN | Permanent Account Number |
| PCA | Prevention of Corruption Act |
| PPI | Prepaid payment instrument(s) |
| PFRDA | Pension Fund Regulatory and Development Authority |
| PMLA | Prevention of Money Laundering Act |
| PML | Prevention of money laundering |

| | DEFINITION |
|---|---|
| PSO | Payment system operator |
| RAMC | Risk Assessment and Monitoring Committee |
| RBI | Reserve Bank of India |
| RE | Reporting Entity(ies) |
| SAARC | South Asian Association for Regional Cooperation |
| SAFEMA | Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act |
| SAG | Strategic analysis group (at the FIU) |
| SAL | Strategic analysis lab (at the FIU) |
| SBO | Significant Beneficial Owner |
| SCOMET | Special Chemicals, Organisms, Materials, Equipment and Technologies |
| SDD | Simplified due diligence |
| SEBI | Securities and Exchange Board of India |
| SFIO | Serious Fraud Investigation Office |
| SMAC | Subsidiary Multi-agency Centre |
| SME | Subject matter expert |
| SoC | Statement of Cooperation |
| SOP | Standard operating procedure |
| SRA | Sectoral Risk Assessment |
| TIEA | Tax Information Exchange Agreement |
| TBML | Trade-based money laundering |
| TF | Terrorist Financing |
| TFS | Targeted financial sanctions |
| UAPA | Unlawful Activities (Prevention) Act |
| UCB | Urban Co-operative Bank |
| UNCAC | The United Nations Convention against Corruption (the 'Merida Convention') |
| UNSC | United Nations Security Council |
| UNSCR | United Nations Security Council Resolution |
| UNTOC | United Nations Convention against Transnational Organised Crime (the 'Palermo Convention') |
| WMD | Weapons of mass destruction |

September 2024

# Anti-money laundering and counter-terrorist financing measures - India

## *Fourth Round Mutual Evaluation Report*

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in India as at the time of the on-site visit from 6-24 November 2023.

The report analyses the level of effectiveness of India's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.