NISM CERTIFICATION EXAMINATION WORK BOOK
XXIV

AML and CFT Provisions in Securities Markets

National Institute of Securities Markets
A Capacity Building Initiative of SEBI

Workbook for

NISM-Series-XXIV: AML and CFT Provisions in Securities Markets Certification Examination

National Institute of Securities Markets
www.nism.ac.in

This workbook has been developed to assist candidates in preparing for the National Institute of Securities Markets (NISM) Certification Examination for AML and CFT Provisions in Securities Markets.

Workbook Version: May 2025[1]

Published by:
National Institute of Securities Markets

NISM Registered Office
5th floor, NCL Cooperative Society,
Plot No. C-6, E-Block, Bandra Kurla Complex,
Bandra East, Mumbai, 400051

National Institute of Securities Markets
Patalganga Campus
Plot IS-1 & IS-2, Patalganga Industrial Area
Village Mohopada (Wasambe)
Taluka-Khalapur
District Raigad-410222.

Website: www.nism.ac.in

[1] Note: The updates made in the workbook (version: May 2025) have been highlighted in YELLOW for easy identification. Kindly refer to the workbook (version: May 2025) for appearing in the NISM Series XXIV: AML and CFT Provisions in Securities Markets Certification Examination on or after June 20, 2025.

Foreword

NISM is a leading provider of high-end professional education, certifications, training and research in financial markets. NISM engages in capacity building among stakeholders in the securities markets, through professional education, financial literacy, enhancing governance standards and fostering policy research.

The NISM certification programs aim at enhancing the quality and standards of professionals employed in various segments of the financial sector. NISM develops and conducts certification examinations and Continuing Professional Education (CPE) programs that aim at ensuring that professionals meet the defined minimum common knowledge benchmark for various critical securities market functions.

NISM certification examinations and educational programs service different securities market intermediaries focusing on varied product lines and functional areas. NISM certifications have established knowledge benchmarks for various market products and functions such as equities, mutual funds, derivatives, compliance, operations, advisory and research. NISM certification examinations and training programs provide a structured learning plan and career path to students and job aspirants, wishing to make a professional career in the securities markets.

NISM supports candidates by providing lucid and focused workbooks that assist them in understanding the subject and preparing for NISM Examinations. This book covers important topics to create awareness among the employees of Associated Persons (APs) registered with stock exchanges and other market intermediaries about Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Provisions in Securities Markets. The book focusses on discussing various regulatory aspects of prevention of money laundering. It discusses the concept such as AML, CFT, PF, scheduled offences; regulatory provisions/guidelines of AML and CFT under the PMLA, SEBI Act, Companies Act, among others. It also provides learners the practical understanding on the implementation and coverage of PMLA through different case studies.

Sashi Krishnan

Director

Disclaimer

The contents of this publication do not necessarily constitute or imply its endorsement, recommendation, or favoring by the National Institute of Securities Markets (NISM) or the Securities and Exchange Board of India (SEBI). This publication is meant for general reading and educational purpose only.

The statements/explanations/concepts are of general nature and may not have taken into account the particular objective/ move/ aim/ need/ circumstances of individual user/ reader/ organization/ institute. Thus, NISM and SEBI do not assume any responsibility for any wrong move or action taken based on the information available in this publication.

Therefore, before acting on or following the steps suggested on any theme or before following any recommendation given in this publication user/reader should consider/seek professional advice.

The publication contains information, statements, opinions, statistics and materials that have been obtained from sources believed to be reliable and the publishers of this title have made best efforts to avoid any errors. However, publishers of this material offer no guarantees and warranties of any kind to the readers/users of the information contained in this publication.

Since the work and research is still going on in all these knowledge streams, NISM and SEBI do not warrant the totality and absolute accuracy, adequacy or completeness of this information and material and expressly disclaim any liability for errors or omissions in this information and material herein. NISM and SEBI do not accept any legal liability whatsoever based on any information contained herein.

While the NISM Certification examination will be largely based on material in this workbook, NISM does not guarantee that all questions in the examination will be from material covered herein.

Acknowledgement

This workbook has been developed jointly by the Certification Team of National Institute of Securities Markets (NISM) and NISM Resource Person—Ms. Monica Sachdeva. It is reviewed by Dr. Shreyas Vyas, NISM faculty in Law. NISM gratefully acknowledges the contribution of the Examination Committee of NISM Series XXIV: AML and CFT Provisions in Securities Markets Certification Examination consisting of industry experts.

About NISM Certifications

The Centre for Capacity Building at NISM is engaged in developing and administering Certification Examinations and CPE Programs for professionals employed in various segments of the Indian securities markets. These Certifications and CPE Programs are being developed and administered by NISM as mandated under Securities and Exchange Board of India (Certification of Associated Persons in the Securities Markets) Regulations, 2007.

The skills, expertise and ethics of professionals in the securities markets are crucial in providing effective intermediation to investors and in increasing the investor confidence in market systems and processes. The Centre for Capacity Building seeks to ensure that market intermediaries meet defined minimum common benchmark of required functional knowledge through Certification Examinations and Continuing Professional Education Programmes on Mutual Funds, Equities, Derivatives Securities Operations, Compliance, Research Analysis, Investment Advice and many more.

Certification creates quality market professionals and catalyzes greater investor participation in the markets. Certification also provides structured career paths to students and job aspirants in the securities markets.

About the Certification Examination of AML and CFT Provisions in Securities Markets

The examination seeks to create a common minimum knowledge benchmark for the employees of securities market intermediaries about Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Provisions in Securities markets.

The examination covers various aspects related to Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF). Some of them are the Prevention of Money Laundering Act, 2002 (PMLA), Scheduled Offences, AML and CFT Guidelines and PMLA related cases.

The certification aims to create awareness among the employees of securities market intermediaries about the AML and CFT Provisions in Securities Markets.

Examination Objectives

On successful completion of the examination, the candidate should:

- Know the concepts of AML and CFT and related aspects, provisions of the PMLA, and scheduled offences under the SEBI Act and the Companies Act.

- Understand guidelines pertaining to Anti Money Laundering (AML) Standards, Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF).

Assessment Structure

The examination consists of 50 questions of 1 mark each and should be completed in 1 hour. The passing percentage for the examination is 50 percent. There shall be no negative marking.

How to register and take the examination

To find out more and register for the examination please visit *www.nism.ac.in*

Syllabus Outline with Weightages

Sr. No.	Chapter Name	Weightage
Part A		
1	Introduction to Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)	6
2	Prevention of Money Laundering Act, 2002 (PMLA)	8
3	The Prevention of Money-laundering (Maintenance of Records) Rules, 2005	8
Part B		
4	Scheduled Offences	3
5	Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF) Guidelines	5
6	SEBI Guidelines for Anti Money Laundering (AML) Standards, Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)	7
7	SEBI guidelines for KYC norms in Securities Market	8
8	Discussion on PMLA related Cases	5
Total Marks		**50**

Contents

_Toc191552536

Chapter-1 Introduction to Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)

Learning Objective- After studying this chapter, you should know about:

- Detailed definition of Money Laundering and Combating the Financing of Terrorism
- All probable sources of illegally gained money (for e.g. arms sales, narcotics, human trafficking, contraband smuggling, embezzlement, insider trading, bribery, and fraud schemes).

1.1. Introduction

A large number of criminal acts aim to generate a profit for the individual or group that carries out the act. Money laundering is the process of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. Illegal arms sales, smuggling, and the activities of organised crime, including drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering.[2]

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. Practice of or engagement in any of such activities is known as Money Laundering.

Money Laundering has devastating social consequences. For one thing, money laundering provides the fuel for un-ethical persons such as drug dealers, terrorists, arms dealers, and other criminals to operate and expand their criminal enterprises. In addition to organized criminal groups, professional money launderers perform money laundering services on behalf of others as their core business. If, left unchecked, money laundering can erode the integrity of our nation's financial institutions. Hence, financial institutions employ anti-money laundering (AML) policies to detect and prevent such activities.

[2] https://fiuindia.gov.in/files/FAQs/faqs.html

1.1.1 Need for Anti Money Laundering Laws (History)

Anti-money laundering (AML) laws are important and much required because they help preventing criminals from hiding illegally obtained money and the financial impact of money laundering on a country, thus safeguarding the financial system from crimes.

Anti-money laundering guidelines came into prominence globally as a result of the formation of the Financial Action Task Force (FATF) and the promulgation of an international framework of anti-money laundering standards. These standards began to have more relevance in 2000 and 2001, after FATF began a process to publicly identify countries that were deficient in their anti-money laundering laws and international cooperation.

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. The provisions of PMLA came into force on July 1, 2005. The objective of PMLA is, "to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto."

1.2. Process of Money Laundering

There are typically three stages[3] of the money laundering process to release laundered funds into the legal financial system. These three stages of money laundering are:

- Placement
- Layering
- Integration/extraction

1.2.1 Money laundering Stages

Stage 1: Placement in the financial system

The placement stage in money laundering is when the illegally obtained funds are introduced in the financial system. This is often done by breaking up large amounts of cash into less conspicuous smaller sums to deposit directly into a bank account or by purchasing monetary instruments such as checks or money orders that are collected and deposited into accounts at other locations. The placement stage of money laundering is full of challenges for the criminals as it involves placing money into the legal system without causing any suspicion.

[3] https://complyadvantage.com/insights/3-stages-money-laundering/

Some placement methods include:

- **Adding illicit cash:** Adding illicit cash from a crime to the legitimate takings of a business, particularly those with little or no variable costs;
- **Smurfing:** Smurfing is where small amounts of money below the AML reporting threshold are inserted into bank accounts or credit cards and used to pay expenses, etc.;
- **Mules[4] or cash smugglers:** Cash is smuggled across borders and deposited into foreign accounts;
- **Hiding Identity:** Hiding the beneficial owner's identity through trusts and offshore companies;
- **Investing in commodities:** Using gems and gold that can be moved easily to other jurisdictions;
- **Buying and Selling:** Using cash for quick turnaround investment in assets such as real estate, cars, and boats;
- **Gambling:** Using casino transactions to launder money
- **Shell companies:** Establishing inactive companies or corporations that exist only on paper.

Stage 2: Layering the funds

The layering stage is when the launderer moves the money through a series of financial transactions with the goal of making it difficult to trace the original source.

The funds could be channeled through the purchase and sales of investments, a holding company, or simply moved through a series of accounts at banks around the globe. Widely scattered accounts are most likely to be found in jurisdictions that do not cooperate with AML investigations. In some instances, the launderer could disguise the transfers as payments for goods or services or as a private loan to another company, giving them a legitimate appearance. Few layering tactics are:

- **Chain-hopping** — converting one digital currency into another and moving from one blockchain to another;
- **Mixing or tumbling** — the blending of various transactions across several exchanges, making transactions harder to trace back to a specific exchange, account, or owner;
- **Cycling** — making deposits of fiat currency from one bank, purchasing and selling digital currency, and then depositing the proceeds into a different bank or account.

[4] As per SEBI PFUTP Regulations, "mule account" includes a trading account maintained with a stock broker or a dematerialised account or bank account linked with such trading account in the name(s) of a person, where the account is effectively controlled by another person, whether or not the consideration for transactions in the account are paid by such other person.

Stage 3: Integration into the legitimate financial system

The integration stage of money laundering is the final step in the laundering process. This is when the launderer attempts to integrate illicitly obtained funds into the legitimate financial system. To use the funds to buy goods and services without attracting attention from law enforcement or the tax authorities, the criminal may invest in real estate, luxury assets, or business ventures.

They are often content to use payroll and other taxes to make the "washing" more legitimate, accepting a 50% "shrinkage" in the wash as the cost of doing business.

Common integration tactics include:

- Fake employees – a way of getting the money back out. Usually paid in cash and collected;
- Loans – to directors or shareholders, which will never be repaid;
- Dividends – paid to shareholders of companies controlled by criminals.

While not all money laundering cases will use all the three-stage process – they could be combined or stages repeated several times, thus the rule of three stages of money laundering frames the thinking of many compliance teams.

1.3. Global initiatives towards Anti Money Laundering Laws

Anti-money laundering Laws are an international web of laws, activities, regulations, and procedures, aimed at uncovering money that has been disguised as legitimate income. For decades, governments and law enforcement agencies have tried to fight crime by following the money, thus aiming to achieve the purpose of the AML Laws which is to help detect and report suspicious activity including the predicate offenses to money laundering and terrorist financing, securities fraud and market manipulation.

Let's understand few Global Initiatives towards AML proceeds by understanding these Laws:

1.3.1 Bank Secrecy Act of 1970 (BSA)

The United States was one of the first nations to enact anti-money laundering legislation when it *enacted* the Bank Secrecy Act (BSA) in 1970. The Bank Secrecy Act of 1970 (BSA), also known as the Currency and Foreign Transactions Reporting Act, requires financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering. The act specifically requires:

- Financial institutions to keep records of cash purchases of negotiable instruments
- File reports if the daily aggregate exceeds $10,000, and
- Report suspicious activity that may signify money laundering, tax evasion, or other criminal activities.

The BSA was originally passed by the U.S. Congress in 1970[5] and signed by President Richard Nixon into law on October 26, 1970. Until the 1980s, there was a prolonged period of inaction on it, but eventually financial institutions complied with its reporting requirements.

The BSA is sometimes referred to as an anti-money laundering law (AML) or jointly as BSA/AML. An early effort to detect and prevent money laundering, the BSA has since been amended and strengthened by additional anti-money laundering laws. The Financial Crimes Enforcement Network is now the designated administrator of the BSA – with a mission to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activities."

1.3.2 Financial Action Task Force (on Money Laundering)- FATF (1989)

The Financial Action Task Force (on Money Laundering)- FATF, also known by its French name, “Grouped' action financière” (GAFI), is an intergovernmental organization founded in 1989 with the initiative of the 1989 G7 Summit in Paris. The mission of FATF is:

- To devise and promote international standards to prevent the growing problem of money laundering;
- Study money laundering trends;
- Monitor legislative, financial and law enforcement activities taken at the national and international level;
- Reporting on compliance, and;
- Issuing recommendations and standards to combat money laundering.

At the time of its formation, FATF had 16 members, which by 2023 had grown to 40[6]. In its first year, FATF issued a report containing forty recommendations to more effectively fight money laundering. These standards were revised in 2023[7] to reflect evolving patterns and techniques in money laundering.

[5]https://www.fincen.gov/history-anti-money-laundering-laws
[6] https://www.fatf-gafi.org/en/countries.html
[7] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html

Shortly after the 9/11 attacks on the US, FATF expanded its mandate to include AML and combating terrorist financing.

India became a member of FATF in 2010. India is also a member of two FATF Style Regional Bodies (FSRBs)- Asia Pacific Group (APG) and Eurasian Group of Combating Money Laundering and Financing of Terrorism (EAG).[8]

The core work of FATF is to conduct Mutual Evaluation of its Members and to guide and assist SRBs to conduct Mutual evaluation of their respective member jurisdictions.

1.3.3 The International Monetary Fund (IMF)

The International Monetary Fund (IMF) is another important organization. With 189 Member countries, its primary purpose is to ensure stability of the international monetary system. The IMF is concerned about the consequences of money laundering and related crimes affecting the integrity and stability of the financial sector and the broader economy.

The IMF has decades of experience in these areas. It has helped shape policies on anti-money laundering (AML) combatting the financing of terrorism (CFT) and counter-proliferation financing internationally and within its members' national frameworks.

The IMF expanded its AML efforts in 2000 and extended them to CFT after the terrorist attacks on September 11, 2001. In 2004, the IMF Executive Board agreed to make AML/CFT assessments and capacity development a regular part of IMF work.

1.3.4 Bank for International Settlements (BIS) Initiative, (1930)

The Bank for International Settlements (BIS) is an international financial institution which is owned by member central banks. Its primary goal is to foster international monetary and financial cooperation while serving as a bank for central banks. With its establishment in 1930, it is the oldest international financial institution. Its initial purpose was to oversee the settlement of World War-I war reparations.

The Bank for International Settlements (BIS) has played a role in anti-money laundering (AML) measures in several ways, including:

- **Providing a forum for cooperation -** The BIS provides a platform for central banks and financial supervisory authorities to exchange information and collaborate.

[8] https://dor.gov.in/fatf and https://www.fatf-gafi.org/en/countries/global-network.html

- **Supporting research and policy analysis -** The BIS conducts research and policy analysis on issues related to monetary and financial stability.
- Acting as a bank for central banks
- The BIS acts as a prime counterparty for central banks in their financial transactions.
- **Issuing guidelines -** The BIS has issued guidelines on sound management of risks related to money laundering.
- **Providing online learning tools -** The BIS offers online learning tools, such as FSI Connect, on AML and CFT in banking.

1.3.5 The Vienna Convention (1988)

Money laundering has been addressed in the UN Vienna 1988 Convention Article 3.1, describing Money Laundering as: *"the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions".*

The Vienna Convention, adopted in December 1988, lays the groundwork for efforts to combat money laundering by creating an obligation for signatory states to criminalize the laundering of money from drug trafficking. It promotes:

- International cooperation in investigations and
- Makes extradition between signatory states applicable to money laundering.

It establishes the principle that domestic bank secrecy provisions should not interfere with international criminal investigations.

1.4. Indian initiatives towards Anti Money Laundering Laws

Anti-money laundering laws in India are a critical aspect of the country's financial and economic framework. They are designed to prevent the illegal flow of funds through the banking and financial system and to promote transparency and accountability in financial transactions. India has implemented a comprehensive set of anti-money laundering laws, which have been updated periodically to keep pace with global best practices. A brief note of these laws is:

1.4.1 Prevention of Money Laundering Act, 2002 (PMLA)

In India, Prevention of Money Laundering Act, 2002 (PMLA) was enacted to fight against the criminal offence of legalizing the income/profits from an illegal source. The act provides for the

prevention, detection, and prosecution of money laundering activities. It requires financial institutions to maintain records of all transactions and report any suspicious activity to the authorities. The Prevention of Money Laundering Act, 2002 enables the government or the public authority to confiscate the property earned from the illegally gained proceeds. This Act, has been dealt in detail in the next chapter.

1.4.2 Unlawful Activities Prevention Act, 1967 (UAPA)

This Act provides more effective prevention of certain unlawful activities of individuals and associations, and for dealing with terrorist activities, and for matters connected therewith. The act empowers the government to ban organizations involved in terrorist activities and freeze their assets. It also provides for severe punishment for those involved in such activities.

1.4.3 Foreign Exchange Management Act, 1999 (FEMA)

This Act consolidates and amends the laws relating to foreign exchange with the objective of facilitating external trade and payments and for promoting the orderly development and maintenance of foreign exchange market in India. The act regulates foreign exchange transactions and prohibits money laundering and financing of terrorism through such transactions.

1.4.4 Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under

The Prevention of Money Laundering Act, 2002 ("PMLA") and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time and notified by the Government of India, mandate every reporting entity which includes intermediaries registered under section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) and stock exchanges, to adhere to client account opening procedures, maintain records and report such transactions as prescribed therein to the relevant authorities. The PML Rules, inter alia, empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by the regulator. The aforesaid guidelines stipulate the essential principles for combating Money Laundering

(ML) and Terrorist Financing (TF) and provide detailed procedures and obligations to be followed and complied with by all the registered intermediaries.

1.4.5 Financial Intelligence Unit (FIU)

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspected financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

The main function of FIU-IND is to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities. The functions of FIU-IND are:

- **Collection of Information**: Act as the central reception point for receiving Cash Transaction reports (CTRs), Non-Profit Organisation Transaction Report (NTRs), Cross Border Wire Transfer Reports (CBWTRs), Reports on Purchase or Sale of Immovable Property (IPRs) and Suspicious Transaction Reports (STRs) from various reporting entities.
- **Analysis of Information**: Analyze received information in order to uncover patterns of transactions suggesting suspicion of money laundering and related crimes.
- **Sharing of Information**: Share information with national intelligence/law enforcement agencies, national regulatory authorities and foreign Financial Intelligence Units.
- **Act as Central Repository:** Establish and maintain national data base on the basis of reports received from reporting entities.
- **Coordination**: Coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.
- **Research and Analysis**: Monitor and identify strategic key areas on money laundering trends, typologies and developments.

The prevention of money laundering is essential to combat financial terrorism effectively. The implementation of robust regulations and guidelines, improved collaboration between financial institutions and governments, and the use of technology-driven solutions are considered crucial to prevent the financing of terrorism. Collective action approach of the institutions aims to combat financial terrorism and ensure global financial stability and security.

Sample Questions

1. Criminals practice money laundering by which of the following ways?
   a) Disguising the source of ill-gotten gains
   b) Changing the form of criminal proceeds
   c) Elsewhere moving profits of criminal acts
   d) All of the above

2. Why are Anti Money Laundering Laws very important for a country?
   a) They help in preventing criminals from hiding illegally obtained money.
   b) They let criminals enjoy the ill-gotten profits.
   c) They have minimum social consequences.
   d) They erode the integrity of a nation's Financial Institutions.

3. What is the stage of money laundering, when the illegally obtained funds are introduced in the financial system, known as?

   a) Extraction
   b) Placement
   c) Layering
   d) Integration

4. The main function of which organisation is to receive cash/suspicious transaction reports, analyse them and, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities.?
   a) RBI
   b) SEBI
   c) FIU-IND
   d) IRDAI

Chapter-2 Prevention of Money Laundering Act, 2002

Learning Objective - After studying this chapter, you should know about:

- Definition, objective and explanation of the concept and importance of Prevention of Money Laundering as per PMLA 2002.
- The penalty provisions for violating the PMLA 2002, as per section 4 of the Act.

2.1 Prevention of Money Laundering Act, 2002 (PMLA)

Prevention of Money Laundering Act (PMLA) forms the core of the legal framework put in place by India to combat money laundering. It is an act to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto. PMLA and the Rules notified there under came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act. The PMLA and rules notified thereunder impose obligation on banking companies, financial institutions, and intermediaries and persons carrying on a designated business or profession, to verify identity of clients, maintain records and furnish information to FIU-IND.

2.1.1 Section 2 of the PMLA 2002

This section defines terms used in the Act

(1) In this Act, unless the context otherwise requires, —

(a) "Adjudicating Authority" means an Adjudicating Authority appointed under sub-section (1) of section 6;

(b) "Appellate Tribunal" means the Appellate Tribunal established under section 25;

(c) "Assistant Director" means an Assistant Director appointed under sub-section (1) of section 49;

(d) "attachment" means prohibition of transfer, conversion, disposition or movement of property by an order issued under Chapter III;

(da) “authorised person” means an authorised person as defined in clause (c) of section 2 of the Foreign Exchange Management Act, 1999(42 of 1999);

(e) “banking company” means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949) applies and includes any bank or banking institution referred to in section 51 of that Act;

(f) “Bench” means a Bench of the Appellate Tribunal;

(fa) “beneficial owner” means 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;

(g) “Chairperson” means the Chairperson of the Appellate Tribunal;

(h) “chit fund company” means a company managing, conducting or supervising, as foreman, agent or in any other capacity, chits as defined in section 2 of the Chit Funds Act, 1982 (40 of 1982);

(ha) “client” means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting;

(i) “co-operative bank” shall have the same meaning as assigned to it in clause (dd) of section 2 of the Deposit Insurance and Credit Guarantee Corporation Act, 1961 (47 of 1961);

(ia) “corresponding law” means any law of any foreign country corresponding to any of the provisions of this Act or dealing with offences in that country corresponding to any of the scheduled offences;

(ib) “dealer” has the same meaning as assigned to it in clause (b) of section 2 of the Central Sales Tax Act, 1956 (74 of 1956);

(j) “Deputy Director” means a Deputy Director appointed under sub-section (1) of section 49;

(k) "Director" or "Additional Director" or "Joint Director" means a Director or Additional Director or Joint Director, as the case may be, appointed under sub-section (1) of section 49;

(l) "financial institution" means a financial institution as defined in clause (c) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934) and includes a chit fund company, a housing finance institution, an authorised person, a payment system operator, a nonbanking financial company and the Department of Posts in the Government of India;

(m) "housing finance institution" shall have the meaning as assigned to it in clause (d) of section 2 of the National Housing Bank Act, 1987 (53 of 1987);

(n) "intermediary" means, —

(i) a stock-broker, sub-broker share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992); or

(ii) an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 (74 of 1952) or any member of such association; or

(iii) intermediary registered by the Pension Fund Regulatory and Development Authority; or

(iv) a recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);

(na) "investigation" includes all the proceedings under this Act conducted by the Director or by an authority authorised by the Central Government under this Act for the collection of evidence;

(o) "Member" means a Member of the Appellate Tribunal and includes the Chairperson;

(p) "money-laundering" has the meaning assigned to it in section 3;

(q) "non-banking financial company" shall have the same meaning as assigned to it in clause (f) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934);

(r) "notification" means a notification published in the Official Gazette;

(ra) "offence of cross border implications", means—

(i) 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 the proceeds of such conduct or part thereof to India; or

(ii) 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. Explanation.—Nothing contained in this clause shall adversely affect any investigation, enquiry, trial or proceeding before any authority in respect of the offences specified in Part A or Part B of the Schedule to the Act before the commencement of the Prevention of Money-laundering (Amendment) Act, 2008

(rb) "payment system" means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them. Explanation. —For the purposes of this clause, "payment system" includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations;

(rc) "payment system operator" means a person who operates a payment system and such person includes his overseas principal.
Explanation. — For the purposes of this clause, "overseas principal" means, —

(A) in the case of a person, being an individual, such individual residing outside India, who owns or controls or manages, directly or indirectly, the activities or functions of payment system in India;

(B) in the case of a Hindu undivided family, Karta of such Hindu undivided family residing outside India who owns or controls or manages, directly or indirectly, the activities or functions of payment system in India;

(C) in the case of a company, a firm, an association of persons, a body of individuals, an artificial juridical person, whether incorporated or not, such company, firm, association of persons, body of individuals, artificial juridical person incorporated or registered outside India or existing as such and which owns or controls or

manages, directly or indirectly, the activities or functions of payment system in India;

(s) "person" includes; —

(i) an individual,

(ii) a Hindu undivided family,

(iii) a company,

(iv) a firm,

(v) an association of persons or a body of individuals, whether incorporated or not,

(vi) every artificial juridical person, not falling within any of the preceding sub-clauses, and

(vii) any agency, office or branch owned or controlled by any of the above persons mentioned in the preceding sub-clauses;

(sa) "person carrying on designated business or profession" means, —

- a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino;
- Inspector-General of Registration appointed under section 3 of the Registration Act, 1908 as may be notified by the Central Government;
- real estate agent, as may be notified by the Central Government;
- dealer in precious metals, precious stones and other high value goods, as may be notified by the Central Government;
- person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as may be notified by the Central Government; or
- person carrying on such other activities as the Central Government may, by notification, so designate, from time-to time;

(sb) "precious metal" means gold, silver, platinum, palladium or rhodium or such other metal as may be notified by the Central Government;

(sc) "precious stone" means diamond, emerald, ruby, sapphire or any such other stone as may be notified by the Central Government;

(t) "prescribed" means prescribed by rules made under this Act;

(u) “proceeds of crime” means 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; Explanation.—For the removal of doubts, it is hereby clarified that "proceeds of crime" include property not only derived or obtained from 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.

(v) “property” 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;
Explanation. —For the removal of doubts, it is hereby clarified that the term “property” includes property of any kind used in the commission of an offence under this Act or any of the scheduled offences;

(va) “real estate agent” means a real estate agent as defined in clause (88) of section 65 of the Finance Act, 1994;

(w) “records” include the records maintained in the form of books or stored in a computer or such other form as may be prescribed;

(wa) “reporting entity” means a banking company, financial institution, intermediary or a person carrying on a designated business or profession; .

(x) “Schedule” means the Schedule to this Act;

(y) “scheduled offence” means—

(i) the offences specified under Part A of the Schedule; or
(ii) the offences specified under Part B of the Schedule if the total value involved in such offences is one crore rupees or more; or
(iii) the offences specified under Part C of the Schedule;

(z)“Special Court” means a Court of Session designated as Special Court under sub-section (1) of section 43;

(za) “transfer” includes sale, purchase, mortgage, pledge, gift, loan or any other form of transfer of right, title, possession or lien;

(zb) “value” means the fair market value of any property on the date of its acquisition by any person, or if such date cannot be determined, the date on which such property is possessed by such person.

(2) Any reference, in this Act or the Schedule, to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provisions of the corresponding law, if any, in force in that area.

2.1.2 Section 3 of the PMLA 2002

This section gives the definition of Offence of Money Laundering. Whosoever, directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering. Further, the Act clarifies that a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely: —
(a)concealment; or
(b) possession; or
(c) acquisition; or
(d) use; or
(e) projecting as untainted property; or
(f) claiming as untainted property, in any manner whatsoever

The process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.

The PMLA is divided in multiple sections. An illustrative list regarding applicability/scope of coverage of these sections[9] is as mentioned below:

Sections	**Scope of Coverage**
Section 1	Short title, extent & Commencement
Section 2	Definitions
Section 3	Offence of Money Laundering
Section 4	Punishment for Money Laundering
Section 5	Attachment of property involved in money-laundering.
Section 11A	Verification of identity by reporting entity
Section 12	Reporting entity to maintain records
Section 12A & 12 AA	Access to Information
Section 13	Powers of the Director
Section 14	No civil or criminal proceedings against reporting entity, its Directors & Employees in certain cases
Section 15	Procedure and manner of furnishing information by reporting entities
Section 26	Appeals to Appellate Tribunal
Section 39	Right of appellant to take assistance of authorised representative and of Government to appoint presenting officers
Section 40	Members etc. to be public servants
Section 41	Civil court not to have jurisdiction
Section 42	Appeal to high court
Section 44	Offences triable by special courts
Section 48	Authorities under the Act
Section 49	Appointment and powers of authorities and other officers
Section 50	Powers of authorities regarding summons, production of documents and to give evidence etc.
Section 54	Certain officers and others to assist in inquiry etc.
Section 56	Agreements with foreign countries
Section 66	Disclosure of information
Section 69	Recovery of Fine or Penalty
Section 73	Power to make Rules
Section 75	Power to remove difficulties

[9]Source: https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html

2.1.3 Section 4 of the PMLA 2002

As per **Section 4 of the PMLA 2002**, "Whoever commits the offence of money-laundering is punishable with rigorous imprisonment for a term which will not be less than three years but which may extend to seven years and shall also be liable to fine.
However, it may be noted that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words “which may extend to seven years”, the words “which may extend to ten years” had been substituted.

2.1.4 Section 5 of the PMLA 2002

As prescribed under **Section 5 of the Act**, where the Director or any other officer not below the rank of Deputy Director authorised by the Director for the purposes of this section, has reason to believe (recorded in writing), on the basis of material in his possession, that--

(a) any person is in possession of any proceeds of crime; and

(b) such proceeds of crime are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to confiscation of such proceeds of crime may, by order in writing, provisionally attach such property for a period not exceeding one hundred and eighty days from the date of the order, in such manner as may be prescribed

2.1.5 Section 12 of the PMLA 2002

As per Section 12 of the PMLA 2002, the requirement for maintenance of records by reporting entities has been specified. According to the section

(1) Every reporting entity is required to—
   (a) maintain a record of all transactions, in such manner as to enable it to reconstruct individual transactions;
   (b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;
   (c) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

(2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

(4) The records referred to in clause (c) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.

2.1.6 Section 56 of the PMLA 2002

As illustrated under **Section 56 of the PMLA 2002** the international co-operation between countries for the purpose of prevention of money laundering has been specified. Accordingly

(1) The Central Government may enter into an agreement with the Government of any country outside India for:

(a) enforcing the provisions of this Act;

(b) exchange of information for the prevention of any offence under this Act or under the corresponding law in force in that country or investigation of cases relating to any offence under this Act, and may, by notification in the Official Gazette, make such provisions as may be necessary for implementing the agreement.

(2) The Central Government may, by notification in the Official Gazette, direct that the application of this Chapter in relation to a contracting State with which reciprocal arrangements have been made, shall be subject to such conditions, exceptions or qualifications as are specified in the said notification.

2.2 Maintenance of records and furnishing of reports to FIU-IND

For effective implementation of the Act, maintenance and reporting of records is an important requirement. Under the PML Rules, Rule 3 – Maintenance of records of transactions, the following transactions have been specified, for which records have to be maintained and reports are to be furnished to FIU-IND[10]:

[10] Source: https://fiuindia.gov.in/files/AML_Legislation/notification.html and https://fiuindia.gov.in/pdfs/downloads/Brochures%20on%20FIU.pdf

(a) All cash transactions of the value of more than rupees 10 lakh or its equivalent in foreign currency.
(b) All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
(c) All transactions involving receipts by non - profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;
(d) 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;
(e) All suspicious transactions, whether or not made in cash, including attempted transactions.
(f) All cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
(g) All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity.

The Suspicious Transaction Report mentioned at para (e) above should be furnished within seven working days on being satisfied that the transaction is suspicious.

The information in respect of immoveable property transactions referred to in (g) above should be furnished to FIU-IND every quarter by the 15th day of the month succeeding the quarter.

All other reports need to be furnished on a monthly basis by the 15th day of the succeeding month.

Further, every reporting entity is necessarily required to furnish information to Director, FIU-IND online in a standard format prescribed for the purpose. For this purpose, the reporting entity has to register itself with FIU-IND.

2.2.1 Suspicious Transaction

Suspicious Transaction means a transaction (including an attempted transaction) whether or not made in cash which, to a person acting in good faith: a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or b) appears to be made in circumstances of unusual or unjustified complexity; or c) appears to have no economic rationale or bona fide purpose; or d) gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.

Designation of officers for ensuring compliance with provisions of PMLA.

Each reporting entity has to appoint certain designated officials to implement the provisions of the Act in the reporting Organisation.

2.2.2 Appointment of a Principal Officer

The Principal Officer is an officer designated by a registered intermediary who should be an officer at the management level. Principal Officer is designated by a reporting entity for the purpose of Section 12 of PMLA. Rule 7 of the PML Rules requires every reporting entity to communicate the name, designation and address of the Principal Officer to the Director, FIU-IND. The Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions.

2.2.3 Appointment of a Designated Director

In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. Designated director is a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules and includes:

(i) the Managing Director or a whole-time Director if the reporting entity is a company,
(ii) the managing partner if the reporting entity is a partnership firm,
(iii) the proprietor if the reporting entity is a proprietorship concern
(iv) the managing trustee if the reporting entity is a trust,
(v) a person or individual who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

2.3 Main Authorities entrusted for investigations[11]

2.3.1 Directorate of Enforcement

The Directorate of Enforcement is a multi-disciplinary organization mandated with investigation of offence of money laundering and violations of foreign exchange laws. The statutory functions of the Directorate include enforcement of following Acts:

[11] Source: https://enforcementdirectorate.gov.in/what-we-do

- The Prevention of Money Laundering Act, 2002 (PMLA):
- The Foreign Exchange Management Act, 1999 (FEMA)
- The Fugitive Economic Offenders Act, 2018 (FEOA)
- Sponsoring agency under COFEPOSA

2.3.2 Financial Intelligence Unit – India (FIU-IND)

FIU-IND was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Sample Questions

1. The PMLA and the Rules notified there under came into force with effect from which date?
   a) July 01' 2005
   b) July 01' 2002
   c) Both of the above
   d) None of the above

2. Which section of The PMLA gives the definition of Offence of Money Laundering?
   a) Section 2
   b) Section 3
   c) Section 4
   d) Section 5

3. As per Section 4 of the PMLA 2002, whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall fall in between
   a) 3-4 years
   b) 4-5 years
   c) 3-7 years
   d) None of the above

4. According to Section 12 of the PMLA 2002, every reporting entity is required to do which of the following activities?
   a) Maintain a record of all transactions
   b) Furnish to the Director, information relating to such transactions
   c) Maintain details related to identity of its clients
   d) All of the above

Chapter-3 The Prevention of Money-laundering (Maintenance of Records) Rules, 2005

Learning Objective- After studying this chapter, you should know about:

- Definition, objective and process of implementation of PML (Maintenance of Records) Rules, 2005
- Detailed explanation of verifying the identity of the client/ true beneficial owner of the assets under Client Due Diligence rules.

3.1 Introduction to the Prevention of Money-laundering (Maintenance of Records) Rules, 2005

An act is a law or the statute which has been passed by the legislature and approved by the President of India. Rules, on the other hand, help in governing laws. Rules are created after an act to define how the act will be implemented and performed. Rules are secondary to the act, and are created to provide flexibility in implementation.

In exercise of the powers conferred by section 73 of the Prevention of Money-Laundering Act, 2002 (15 of 2003), the Central Government in consultation with the Reserve Bank of India, hereby made the following rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries. Further, vide Gazette Notification dated 7th March, 2023, the above mentioned rules were amended and to be called as the Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2023.

The rules require entities to:

- Develop internal controls: Create policies, procedures, systems, and controls to prevent financial crimes
- Conduct customer due diligence: Follow a process before onboarding customers or executing transactions
- Report suspicious activity: Report suspicious transactions and other specified activities
- Maintain client identity records: Keep records of client identity for ten years after the client stops transacting with the entity.

Thus, we may understand that by mandating robust customer verification, due diligence and reporting practices, SEBI and RBI aim to create a secure environment within the financial sector to prevent illicit financial activities.

3.2 Maintenance of Records of Transactions

3.2.1 Maintenance of Records of Transactions (Nature and Value) (Rule 3)

Rule 3 of PMLR, 2005 is important because it outlines the responsibilities of reporting entities, their officers, and employees in maintaining information. The rule states:

Every reporting entity shall maintain the record of all transactions including, the record of -

(A) all cash transactions of the value of more than ten lakhs rupees or its equivalent in foreign currency;

(B) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

(BA) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;

(C) 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;

(D) all suspicious transactions whether or not made in cash and by way of -

(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) travelers cheques,

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 payment orders, cashiers, cheques, demand drafts, telegraphic or wire transfers, electronic remittances or transfers, internet transfers, Automated Clearing House remittances, lock box driven transfers or remittances, remittances for credit or loading to electronic cards or 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, interbank 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.

(E) all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

(F) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

Rule 3A Implementation of policies by groups:

As per Rule 3A,

(1) Every reporting entity, which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(2) Groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of the Prevention of Money Laundering Act, 2002.

3.2.2 Records Containing Information (Rule 4)

The records referred to in rule 3 shall contain all necessary information specified by the regulator to permit reconstruction of individual transaction including the following information: -

(a) the nature of the transactions
(b) the amount of the transaction and the currency in which it was denominated
(c) the date on which the transaction was conducted; and
(d) the parties to the transaction.

3.2.3 Procedure and Manner of Maintaining Information (Rule 5)

(1) Every reporting entity shall maintain information in respect of transactions with its client referred to in rule 3 in accordance with the procedure and manner as may be specified by its regulator from time to time.

(2) Every reporting entity shall evolve an internal mechanism for maintaining such information in such form and manner and at such intervals as may be specified by its regulator from time to time.

(3) It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of maintaining information as specified by its regulator under sub-rule (1).

3.2.4 Procedure and manner of furnishing information (Rule 7)

(1) Every reporting entity shall communicate to the Director the name, designation and address of the Designated Director and the Principal Officer.
(2) The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity. A copy of such information shall be retained by the Principal Officer for the purposes of official record.
(3) Every reporting entity shall evolve an internal mechanism having regard to any guidelines issued by the Director in consultation with, its regulator, for detecting the transactions referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by the Director in consultation with, its Regulator.
(4) It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of furnishing information as specified by the Director in consultation with, its Regulator.

3.2.5 Furnishing of information to the Director (Rule 8)

(1) The Principal Officer of a reporting entity shall furnish the information in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 every month to the Director by the 15th day of the succeeding month.
(2) The Principal Officer of a reporting entity shall furnish the information promptly in writing or by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 not later than seven working days on being satisfied that the transaction is suspicious.
(3) The Principal Officer of a reporting entity shall furnish, the information in respect of transactions referred to in clause (F) of sub-rule (1) of rule 3, every quarter to the Director by the 15th day of the month succeeding the quarter.
(4) For the purpose of this rule, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-reported transaction beyond the time limit as specified in this rule shall constitute a separate violation.
(5) Notwithstanding anything contained in sub-rule (1) and (3) the Reporting Officer shall furnish the information in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub rule (1) of rule 3 for the months of March 2020, April 2020 and May 2020,

and in respect of transactions referred to in clauses (F) of sub rule (1) of rule 3 for the quarter January-March 2020) by the 30th June, 2020.

3.2.6 Client Due Diligence (Rule 9)

(1) Every reporting entity shall:

a) at the time of commencement of an account-based relationship:

i. identify its clients, verify their identity, obtain information on the purpose and intended nature of the business relationship; and

ii. determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner:

Provided that where the Regulator is of the view that money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business, the Regulator may permit the reporting entity to complete the verification as soon as reasonably practicable following the establishment of the relationship; and

b) in all other cases, verify identity while carrying out:

i. transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or

ii. any international money transfer operations:

Provided that where a client is subscribing or dealing with depository receipts or equity shares, issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is a resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in the sub-rules (3) to (9) of these rules shall be applicable for due-diligence of such beneficial owner.

Explanation - For the purposes of this proviso, the expression "equity share" means a share in the equity share capital of a company and equity share capital shall have the

same meaning as assigned to it in the Explanation to section 43 of the Companies Act, 2013.

(1A) Subject to the provisions of sub-rule (1), every reporting entity shall within ten days after the commencement of an account-based relationship with a client, file the electronic copy of the client's KYC records with the Central KYC Records Registry;

(1B) The Central KYC Records Registry shall process the KYC records received from a reporting entity for de-duplicating and issue a KYC Identifier for each client to the reporting entity, which shall communicate the KYC Identifier in writing to their client;

(1C) Where a client, for the purposes of clause (a) and clause (b), submits a KYC Identifier to a reporting entity, then such reporting entity shall retrieve the KYC records online from the Central KYC Records Registry by using the KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless-

i. there is a change in the information of the client as existing in the records of Central KYC Records Registry;

ii. the current address of the client is required to be verified;

iii. the reporting entity considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

(1D) A reporting entity after obtaining additional or updated information from a client under sub-rule (IC), shall as soon as possible furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client;

(1E) The reporting entity which performed the last KYC verification or sent updated information in respect of a client shall be responsible for verifying the authenticity of the identity or address of the client;

(1F) A reporting entity shall not use the KYC records of a client obtained from the Central KYC Records Registry for purposes other than verifying the identity or address of the client

and shall not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or by the Regulator or by the Director;

(1G) The regulator shall issue guidelines to ensure that the Central KYC records are accessible to the reporting entities in real time.

(2) For the purpose of clause (a) of sub-rule (1), a reporting entity may rely on a third party subject to the conditions that-

(a) the reporting entity, within two days, obtains from the third party or from the Central KYC Records Registry records or the information of the client due diligence carried out by the third party.

(b) the reporting entity takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

(c) the reporting entity is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

(d) the third party is not based in a country or jurisdiction assessed as high risk;

(e) the reporting entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable; and

(f) where a reporting entity relies on a third party that 1s part of the same financial group, the Regulator may issue guidelines to consider any relaxation in the conditions (a) to (d).

(3) The beneficial owner for the purpose of sub-rule (1) shall be determined as under—

(a) where the client is a company, 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.

Explanation. — For the purpose of this sub-clause—

- *"Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;*
- *"Control" shall include 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*

(b) where the client is a partnership firm, the beneficial owner is the natural person, who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.
Explanation - For the purpose of this clause, "Control" shall include the right to control the management or policy decision;

(c) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals

(d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official

(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, 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; and

(f) 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 notified by the Central Government, 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.

(4) Where the client is an individual, he shall for the purpose of sub-rule (1) submit to the reporting entity, -
(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any officially valid document or the equivalent e-document thereof containing the details of his identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the reporting entity

(5) Notwithstanding anything contained in sub-rule (4) and as an alternative thereto, an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account:

Provided that -

(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence. However, if the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

(ii) a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits

on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place.

(iii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty-four months.

(iiia) Notwithstanding anything contained in clause (iii), the small account shall remain operational between 1st April, 2020 and 30th June 2020 and such other periods as may be notified by the Central Government.

(iv) the small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high-risk scenarios, the identity of client shall be established as per the provisions of sub-rule (4):

(v) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established as per the provisions of sub-rule (4).

(6) Where the client is a company, it shall for the purposes of sub-rule (1) submit to the reporting entity one certified copy of the following documents or the equivalent e-documents thereof: -

(i) Certificate of incorporation
(ii) Memorandum and Articles of Association;
(iii) Permanent Account Number of the company;
(iv) a resolution from the Board of Directors, power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf;
(v) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf;
(vi) the names of the relevant persons holding senior management position and;
(vii) the registered office and the principal place of its business, if it is different.

(7) Where the client is a partnership firm, it shall, for the purposes of sub-rule (1), submit to the reporting entity the certified copies of the following documents or the equivalent e-documents thereof, namely: -

i. registration certificate,
ii. partnership deed,
iii. Permanent Account Number of the partnership firm
iv. such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf; and
v. the names of all the partners and address of the registered office, and the principal place of its business, if it is different.

(8) Where the client is a trust, it shall, for the purposes of sub-rule (1) submit to the reporting entity one certified copy of the following documents, namely or the equivalent e-documents thereof: -

i. registration certificate,
ii. trust deed;
iii. Permanent Account Number or Form No.60 of the trust;
iv. such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf,
v. the names of the beneficiaries, trustees, settlor or and authors of the trust and the address of the registered office of the trust; and
vi. list of trustees and documents as are required for individuals under sub-rule (4) for those discharging roles as trustee and authorised to transact on behalf of the trust.

(9) Where the client is an unincorporated association or a body of individuals, it shall submit to the reporting entity one certified copy of the following documents or the equivalent e-documents thereof: -

(i) resolution of the managing body of such association or body of individuals;
(ii) power of attorney granted to him to transact on its behalf;
(iii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;
(iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf; and

(v) such information as may be required by the reporting entity to collectively establish the existence of such association or body of individuals.

(9A) Every Banking Company or Financial Institution or intermediary, as the case may be, shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and a reporting entity has ended or the account has been closed, whichever is later.

(9B) Where the client has submitted any documents for the purpose of sub-rule (1), it shall submit to the reporting entity any update of such documents, for the purpose of updating the records mentioned under sub-rules (4), (5), (6), (7), (8) or (9), as the case may be, within 30 days of such updation.

(10) Where the client purports to act on behalf of juridical person or individual or trust, the reporting entity shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.
In case of a trust, the reporting entity shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clause (b) of sub-rule (1) rule9.

(11) No reporting entity shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

(12) It has following three clauses:
(i) Every reporting entity shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with the knowledge of the client, his business and risk profile and where necessary, the source of funds.
(ii) When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data, the reporting entity shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be.

(iii) The reporting entity shall apply client due diligence measures also 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.

(13) Every reporting entity shall -

(i) carry out 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 that is consistent with any national risk assessment conducted by a body or authority duly notified by the Central Government.

(ii) the risk assessment mentioned in clause (i) shall

(a) be documented

(b) consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied

(c) be kept up to date; and

(d) be available to competent authorities and self-regulating bodies.

(14) (i) The regulator shall issue guidelines incorporating the requirements of sub-rules (1) to (13), sub-rule (15) and sub-rule (17) and may prescribe enhanced or 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.

Explanation-For the purpose of this clause, 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.

(ia) The guidelines issued under clause (i) shall also include appropriate-

(A) exemptions, limitations and conditions and alternate and viable means of identification, to provide account based services to clients who are unable to undergo biometric authentication;

(B) relaxation for continued operation of accounts for clients who are unable to provide Permanent Account Number or Form No. 60; and

(C) exemption, limitations and conditions and alternate and viable means of identification, to provide account based services of clients who are unable to undergo Aadhaar authentication for receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016);

owing to injury, illness or infirmity on account of old age or otherwise, and such like causes.

(ii) Every reporting entity shall formulate and implement a Client Due Diligence Programme, incorporating the requirements of sub-rules (1) to (13) 23, sub-rule (15) and sub-rule (17) and guidelines issued under clause (i) and (ia).

(iii) the Client Due Diligence Programme shall 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.

(15) Where the client has submitted –

(a) his Aadhaar number under clause (a) of sub-rule (4) to the banking company or a reporting entity notified under first proviso to sub-section (1) of section 11A, such banking company or reporting entity shall carry out authentication of the client's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India;

(b) proof of possession of Aadhaar under clause (aa) of sub-rule (4) where offline verification can be carried out, the reporting entity shall carry out offline verification;

(c) an equivalent e-document of any officially valid document, the reporting entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo in the manner specified by the regulator.

(d) any officially valid document or proof of possession of Aadhaar number under clause (ab) of sub-rule (4) where offline verification cannot be carried out, the reporting entity shall carry out verification through digital KYC.

Further, for a period not beyond such date as may be notified for a class of reporting entity, instead of carrying out digital KYC, the reporting entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the officially valid document and a recent photograph where an equivalent e-document is not submitted.

Explanation. — Obtaining a certified copy by the reporting entity shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity as per the provisions contained in the Act.

(16) Every reporting entity shall, where its client submits a proof of possession of Aadhaar Number containing Aadhaar number, ensure such client redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15).

(17) (i) A client already having an account based relationship with a reporting entity, shall submit his Permanent Account Number or the equivalent e-documents thereof or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily cease to be operational till the time the Permanent Account Number or the equivalent e-documents thereof or Form No. 60 is submitted by the client:

Further, before temporarily ceasing operations for an account, the reporting entity shall give the client an accessible notice and a reasonable opportunity to be heard.

Explanation. – For the purpose of this clause, "temporary ceasing of operations" in relation to an account means the temporary suspension of all transactions or activities in relation to that account by the reporting entity till such time the client complies with the provisions of this clause;

(ii) if a client having an existing account based relationship with a reporting entity gives in writing to the reporting entity that he does not want to submit his Permanent Account Number or the equivalent e-documents thereof or Form No.60, as the case may be, the client's account with the reporting entity shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the client in the manner as may be determined by the regulator.

(18) In case of officially valid document furnished by the client does not contain updated address, the following documents or the equivalent e-documents thereof shall be deemed to be officially valid documents for the limited purpose of proof of address: -

(a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill)

(b) property or Municipal tax receipt

(c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address

(d) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation:

Further, the client shall submit updated officially valid document or the equivalent e-documents thereof with current address within a period of three months of submitting the above documents.

(19) Where a client has provided his Aadhaar number for identification under clause (a) of sub-rule (4) and wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the reporting entity.

Functions and obligations of the Central KYC Records Registry (Rule 9A)

(1) The Central Government shall within a period of one hundred and eighty days from the date of coming into force of the Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2015 set-up a Central KYC Records Registry having its own seal for the purpose of receiving, storing, safeguarding and retrieving electronic copies of KYC records obtained by the reporting entities from their clients in accordance with these rules. However in an International Financial Services Centre, no such receiving, storing, safeguarding and retrieving of records shall be required for a client who is a foreign national.

(2) The Central KYC Registry shall perform the following functions and obligations, namely: —

(a) shall follow any operating instructions issued by the Regulator, consistent with the guidelines referred to in clause (g) and issue the same to implement the requirements of these rules;

(b) shall be responsible for storing, safeguarding and retrieving the KYC records and making such records available online to reporting entities or Director.

(c) shall take all precautions necessary to ensure that the electronic copies of KYC records are not lost, destroyed or tampered with and that sufficient back up of electronic records are available at all times at an alternative safe and secure place.

(d) shall cause an annual audit of its controls, systems, procedures and safeguards and shall undertake corrective actions for deficiencies, if any.

(e) shall provide information only to the reporting entities which are registered with it on payment of fees as specified by the regulator.

(f) shall appoint a compliance officer who shall be responsible for monitoring the compliance of the Act, the rules made and the notifications issued thereunder and also the guidelines and instructions issued by the Central Government and the Regulator and for redressal of client's grievances. The compliance officer shall immediately and independently report to the Central Government any noncompliance observed by him.

(g) the Regulator in consultation with the Central Government and the Central KYC Records Registry may issue guidelines to be followed by the reporting entities for filing the KYC records with the Central KYC Records Registry.

(h) the Central Government, in consultation with Regulator, may by notification in the public interest and in the interest of the regulated entities, direct that any of the provisions of rule 9 or rule 9A, —

(i) shall not apply to a class or classes of regulated entities.

(ii) shall apply to the class or classes of regulated entities with exceptions, modifications and adaptations.

3.3 Digital Know Your Customer (KYC) Procedure

A. The reporting entities shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated Application of the Reporting Entities.

B. The access of the Application shall be controlled by the Reporting Entities and it should be ensured that the same is not used by unauthorized persons. The Application shall be

accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Reporting Entities to its authorized officials.

C. The client, for the purpose of KYC, shall visit the location of the authorized official of the Reporting Entity or vice-versa. The original Officially Valid Document (OVD) shall be in possession of the client.

D. The Reporting Entity must ensure that the Live photograph of the client is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Reporting Entity shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Reporting Entities) and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the client.

E. The Application of the Reporting Entities shall have the feature that only live photograph of the client is captured and no printed or video-graphed photograph of the client is captured. The background behind the client while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the client.

F. Similarly, the live photograph of the original officially valid document or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the client and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the client. In those documents where, Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to client's own mobile number. Upon successful validation of the OTP, it will be treated as client signature on CAF. However, if the client does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the Reporting Entity shall not be used for client signature. The Reporting Entity must check that the mobile number used in client signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of client and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Reporting Entity. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Reporting Entity, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to client for future reference.

L. The authorized officer of the Reporting Entity shall check and verify that: -
   i. information available in the picture of document is matching with the information entered by authorized officer in CAF.
   ii. live photograph of the client matches with the photo available in the document.; and
   iii. all of the necessary details in CAF including mandatory field are filled properly.

M. On Successful verification, the CAF shall be digitally signed by authorized representative of the Reporting Entity who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Sample Questions

1. After an Act has been passes and approved, its subsequent rules are made for what purpose?
   a) To define how the Act will be implemented
   b) To state how the Act will be performed
   c) To provide flexibility in the implementation of the Act
   d) All of the above

2. The PML (Maintenance of Records) Rules, 2005 require the reporting entities to take which of the following actions?
   a) Report suspicious transactions and other specified activities
   b) Ignore suspicious transactions and other specified activities
   c) Delay suspicious transactions and other specified activities
   d) None of these

3. Every reporting entity shall maintain the record of all cash transactions of value more than a specified amount or its equivalent in foreign currency. What is this specified/threshold amount?
   a) 5 lacs
   b) 10 lacs
   c) 20 lacs
   d) 25 lacs

4. For the purpose of receiving, storing, safeguarding and retrieving electronic copies of KYC records, within how many days of coming into force of the Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2005, a Central KYC Records Registry had to be set up?
   a) 100 days
   b) 150 days
   c) 180 days
   d) 200 days

Chapter - 4 Scheduled Offences

Learning Objective- After studying this chapter, you should know about:

- scheduled offenses described under the SEBI Act and the Companies Act.

4.1 The Concept of Offence

The term offence is better known as "a crime or an illegal action". In order to proceed against a person under the PMLA, a scheduled offence, as defined under section 2(1)(y) and mentioned in Parts A, B and C of the Schedule of the PMLA 2002 should have been committed and the proceeds of crime should have been generated. A critical element, for an offence to be termed as a money laundering offence is the commission of a scheduled offence, as it serves as the foundation for generating proceeds of crime.

The offence of money laundering arises from criminal activity committed by a person in relation to scheduled offences. Scheduled offences (as defined in section 2(1)(y) of the PML Act) are those offences that are mentioned in Parts A, B and C of the Schedule to the PML Act and refer to any type of property or assets derived from proceeds of crime or used in the commission of crime in relation with the scheduled offences.

4.2 List of Scheduled Offences

Part A of the PMLA delineates an exhaustive list of scheduled offences drawn from various criminal legislations in India, including but not limited to the:

- Bharatiya Nyaya Sanhita (BNS) 2023 (erstwhile Indian Penal Code 1860),
- Narcotic Drugs and Psychotropic Substances Act 1985,
- Unlawful Activities (Prevention) Act 1967,
- Arms Act 1959,
- Prevention of Corruption Act 1988, and others, for which no monetary threshold has been provided.
- Antiquities and Art Treasures Act
- Copyright Act
- Trademark Act
- Wildlife Protection Act
- Information Technology Act

In addition to offences mentioned in Part A, **Part B** also encompasses offences under Indian tax laws, such as the Customs Act 1962, for which a monetary threshold of 3 million rupees or 10 million rupees has been prescribed as may be applicable.

Further, **Part C** of the PMLA specifies that any offence mentioned under Part A, particularly offences with cross-border implications, falls within the purview of the Act for which no monetary threshold has been provided.

List of scheduled offences is as follows[12]:

PART A		
Paragraph 1		
Offences Under the Indian Penal Code (45 of 1860) and under Bharatiya Nyaya Sanhita (BNS) 2023 (45 of 2023)		
Section under IPC	**Section under BNS**	**Description of Offence**
120 B	61(2)	Criminal conspiracy.
121	147	Waging, or attempting to wage war or abetting waging of war, against the Government of India.
121A	148	Conspiracy to commit offences punishable by section 121 against the State
255	178	Counterfeiting Government stamp.
257	181	Making or selling instrument for counterfeiting Government stamp.
258	179	Sale of counterfeiting Government stamp.
259	180	Having possession of counterfeit Government stamp.
260	179	Using as genuine a government stamp known to be counterfeit.
302	103(1)	Murder
304	105	Punishment for culpable homicide not amounting to murder.
307	109	Attempt to murder.
308	110	Attempt to commit culpable homicide.
327	119(1)	Voluntarily causing hurt to extort property, or to constrain to an illegal act.
329	119(2)	Voluntarily causing grievous hurt to extort property, or to

[12] https://fiuindia.gov.in/files/AML_Legislation/scheduled_offences.html

		constrain to an illegal act.
364A	140(2)	Kidnapping for ransom, etc.
384 to 389	308	Offences relating to extortion
392 to 402	310 - 313	Offences relating to robbery and dacoity.
411	317(2)	Dishonestly receiving stolen property.
412	317(3)	Dishonestly receiving property stolen in the commission of a dacoity.
413	317 (4)	Habitually dealing in stolen property.
414	317(5)	Assisting in concealment of stolen property.
417	318 (2)	Punishment for cheating.
418	318 (3)	Cheating with knowledge that wrongful loss may ensure to person whose interest offender is bound to protect.
419	319 (2)	Punishment for cheating by personation.
420	318 (4)	Cheating and dishonesty inducing delivery of properties
421	320	Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors.
422	321	Dishonestly or fraudulently preventing debt being available for creditors.
423	322	Dishonest or fraudulent execution of deed of transfer containing false statement of consideration.
424	323	Dishonest or fraudulent removal or concealment of property.
467	338	Forgery of a valuable security, will, etc.
471	340(2)	Using as genuine a forged document or electronic record.
472 and 473	341 (1) & (2)	Making or possessing counterfeit seal, etc. with intent to commit forgery.
475 and 476	342	Counterfeiting device or mark.
481	345(2)	Using a false property mark.
482	345 (3)	Punishment for using false property mark.
483	347 (1)	Counterfeiting a property mark used by another.
484	347 (2)	Counterfeiting a mark used by a public servant.
485	348	Making or possession of any instrument for counterfeiting a property mark.
486	349	Selling goods marked with a counterfeit property mark.
487	350 (1)	Making a false mark upon any receptacle containing goods.
488	350 (2)	Punishment for making use of false mark.;

489A	178	Counterfeiting currency notes or bank notes.
489B	179	Using as genuine, forged or counterfeit currency notes or bank notes

Paragraph 2	
Offences under The Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985)	
Section	**Description of Offence**
15	Contravention in relation to poppy straw.
16	Contravention in relation to coca plant and coca leaves.
17	Contravention in relation to prepared opium.
18	Contravention in relation to opium poppy and opium
19	Embezzlement of opium by cultivator
20	Contravention in relation to cannabis plant and cannabis.
21	Contravention in relation to manufactured drugs and preparations
22	Contravention in relation to psychotropic substances
23	Illegal import into India, export from India or transhipment of narcotic drugs and psychotropic substances.
24	External dealings in narcotic drugs and psychotropic substances in contravention of section 12 of the Narcotics Drugs and Psychotropic Substances Act, 1985.
25A	Contravention of orders made under section 9A of the Narcotic Drugs and Psychotropic Substances Act, 1985
27A	Financing illicit traffic and harbouring offenders.
29	Abetment and criminal conspiracy.

Paragraph 3	
The Explosive Substances Act, 1908 (6 of 1908)	
Section	**Description of Offence**
3	Causing explosion likely to endanger life or property.
4	Attempt to cause explosion, or for making or keeping explosives with intent to endanger life or property.
5	Making or possessing explosives under suspicious circumstances.

Paragraph 4	
The Unlawful Activities (Prevention) Act, 1967 (37of 1967)	
Section	**Description of Offence**
10 read with	Penalty for being member of an unlawful association, etc.

section 3	
11 read with sections 3 and 7	Penalty for dealing with funds of an unlawful association
13 read with section 3	Punishment for unlawful activities.
16 read with section 15	Punishment for terrorist act
16A	Punishment for making demands of radioactive substances, nuclear devices, etc.
17	Punishment for raising fund for terrorist act.
18	Punishment for conspiracy, etc.
18A	Punishment for organising of terrorist camps.
18B	Punishment for recruiting of any person or persons for terrorist act
19	Punishment for harbouring, etc.
20	Punishment for being member of terrorist gang or organization.
21	Punishment for holding proceeds of terrorism.
38	Offence relating to membership of a terrorist organization.
39	Offence relating to support given to a terrorist organization
40	Offence for raising fund for a terrorist organization
Paragraph 5	
The Arms Act, 1959	
Section	**Description of Offence**
25	To manufacture, sell, transfer, convert, repair or test or prove or expose or offer for sale or transfer or have in his possession for sale, transfer, conversion, repair, test or proof, any arms or ammunition in contravention of section 5 of the Arms Act, 1959
	To acquire, have in possession or carry any prohibited arms or prohibited ammunition in contravention of section 7 of the Arms Act, 1959.
	Contravention of section 24A of the Arms Act, 1959 relating to prohibition as to possession of notified arms in disturbed areas, etc.
	Contravention of section 24B of the Arms Act, 1959 relating to prohibition as to carrying of notified arms in or through public places in disturbed areas.
	Other offences specified in section 25.
26	To do any act in contravention of any provisions of section 3, 4, 10 or 12 of the

	Arms Act, 1959 in such manner as specified in sub-section (1) of section 26 of the said Act etc.
	To do any act in contravention of any provisions of section 5, 6, 7 or section 11 of the Arms Act, 1959 in such manner as specified in sub-section (2) of section 26 of the said Act.
	Other offences specified in section 26.
27	Use of arms or ammunitions in contravention of section 5 or use of any arms or ammunition in contravention of section 7 of the Arms Act, 1959.
28	Use and possession of fire arms or imitation fire arms in certain cases.
29	Knowingly purchasing arms from unlicensed person or for delivering arms, etc., to person not entitled to possess the same.
30	Contravention of any condition of a licence or any provisions of the Arms Act, 1959 or any rule made thereunder.
Paragraph 6	
The Wild Life (Protection) Act, 1972 (53 of 1972)	
Section	**Description of Offence**
51 read with section 9	Hunting of wild animals
51 read with section 17A	Contravention of provisions of section 17A relating to prohibition of picking, uprooting, etc., of specified plants.
51 read with section 39	Contravention of provisions of section 39 relating to wild animals, etc., to be Government property.
51 read with section 44	Contravention of provisions of section 44 relating to dealings in trophy and animal articles without licence prohibited.
51 read with section 48	Contravention of provisions of section 48 relating to purchase of animal, etc., by licensee
51 read with section 49B	49B Contravention of provisions of section 49B relating to prohibition of dealings in trophies, animal articles etc., derived from scheduled animals.
Paragraph 7	
The Immoral Traffic (Prevention) Act, 1956 (104 of 1956)	
Section	**Description of Offence**
5	Procuring, inducing or taking person for the sake of prostitution.
6	Detaining a person in premises where prostitution is carried on.
8	Seducing or soliciting for purpose of prostitution.
9	Seduction of a person in custody.

Paragraph 8	
The Prevention of Corruption Act, 1988 (49 of 1988)	
Section	**Description of Offence**
7	Public servant taking gratification other than legal remuneration in respect of an official act.
8	Taking gratification, in order, by corrupt or illegal means, to influence public servant.
9	Taking gratification, for exercise of personal influence with public servant.
10	Abetment by public servant of offences defined in section 8 or section 9 of the Prevention of Corruption Act, 1988
13	Criminal misconduct by a public servant.;
Paragraph 9	
The Explosives Act, 1884 (4 of 1884)	
Section	**Description of Offence**
9-B	Punishment for certain offences
9-C	Offences by Companies.
25 read with section 3	Contravention of export trade in antiquities and art treasure.
28	Offences by Companies.
25 read with section 3	Contravention of export trade in antiquities and art treasure
Paragraph 10	
The Antiquities and Arts Treasures Act, 1972 (52 of 1972)	
Section	**Description of Offence**
25 read with section 3	Contravention of export trade in antiquities and art treasure.
28	Offences by Companies.
Paragraph 11	
The Securities and Exchange Board of India Act, 1992 (15 of 1992)	
Section	**Description of Offence**
12A read with section 24	Prohibition of manipulative and deceptive devices, insider trading and substantial acquisition of securities or control.
24	Acquisition of Securities or Control.

Paragraph 12	
The Customs Act, 1962 (52 of 1962)	
Section	**Description of Offence**
135	Evasion of duty or prohibitions
Paragraph 13	
The Bonded Labour System (Abolition) Act, 1976 (19 of 1976)	
Section	**Description of Offence**
16	Punishment for enforcement of bonded labour.
18	Punishment for extracting bonded labour under the bonded labour system.
20	Abetment to be an offence.
Paragraph 14	
The Child Labour (Prohibition and Regulation) Act, 1986 (61 of 1986))	
Section	**Description of Offence**
14	Punishment for employment of any child to work in contravention of the provisions of section 3.
Paragraph 15	
The Transplantation of Human Organs Act, 1994 (42 of 1994)	
Section	**Description of Offence**
18	Punishment for removal of human organ without authority.
19	Punishment for commercial dealings in human organs.
20	Punishment for contravention of any other provision of this Act.
Paragraph 16	
The Juvenile Justice (Care and Protection of Children) Act,2000 (56 of 2000)	
Section	**Description of Offence**
23	Punishment of cruelty to juvenile or child.
24	Employment of juvenile or child for begging.
25	Penalty for giving intoxicating liquor or narcotic drug or psychotropic substance to juvenile or child.
26	Exploitation of juvenile or child employee.
Paragraph 17	
The Emigration Act,1983 (31 of 1983)	
Section	**Description of Offence**
24	Offences and penalties.
Paragraph 18	

The Passport Act,1967 (15 of 1967)	
Section	**Description of Offence**
12	Offences and penalties.
Paragraph 19	
The Foreigners Act,1946 (31 of 1946)	
Section	**Description of Offence**
14	Penalty for contravention of provisions of the Act, etc.
14B	Penalty for using forged passport.
14C	Penalty for abetment
Paragraph 20	
The Copyright Act,1957 (14 of 1957)	
Section	**Description of Offence**
63	Offence of infringement of copyright or other rights conferred by this Act.
63A	Enhanced penalty on second and subsequent convictions.
63B	Knowing use of infringing copy of computer programme.
68A	Penalty for contravention of section 52A.
Paragraph 21	
The Trade Marks Act,1999 (47 of 1999)	
Section	**Description of Offence**
103	Penalty for applying false trademarks, trade description, etc.
104	Penalty for selling goods or providing services to which false trademark or false trade description is applied.
105	Enhanced penalty on second or subsequent conviction.
107	Penalty for falsely representing a trade mark as registered.
120	Punishment of abetment in India of acts done out of India.
Paragraph 22	
The Information Technology Act, 2000 (21 of 2000)	
Section	**Description of Offence**
72	Penalty for breach of confidentiality and privacy.
75	Act to apply for offence or contravention committed outside India
Paragraph 23	
The Biological Diversity Act,2002 (18 of 2003)	
Section	**Description of Offence**
55 read with	Penalties for contravention of section 6, etc.

6	
Paragraph 24	
The Protection of Plant Varieties and Farmers' Rights Act,2001 (53 of 2001)	
Section	**Description of Offence**
70 read with section 68	Penalty for applying false denomination, etc.
71 read with section 68	Penalty for selling varieties to which false denomination is applied.
72 read with section 68	Penalty for falsely representing a variety as registered.
73 read with section 68	Penalty for subsequent offence.
Paragraph 25	
The Environment Protection Act,1986 (29 of 1986)	
Section	**Description of Offence**
15 read with section 7	Penalty for discharging environmental pollutants.
15 read with section 8	Penalty for handling hazardous substance.
Paragraph 26	
The Water (Prevention and Control of Pollution) Act,1974 (6 of 1974)	
Section	**Description of Offence**
41(2)	Penalty for pollution of stream or well.
43	Penalty for contravention of provisions of section 24.
Paragraph 27	
The Air (Prevention and Control of Pollution) Act,1981 (14 of 1981)	
Section	**Description of Offence**
37	Failure to comply with the provisions for operating industrial plant.
Paragraph 28	
The Suppression of Unlawful Acts Against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002 (69 of 2002)	
Section	**Description of Offence**
3	Offences against ship, fixed platform, cargo of a ship, maritime navigational facilities, etc.

Paragraph 29	
Offence under the Companies Act, 2013	
Section	**Description of Offence**
447	Punishment for fraud

PART B	
OFFENCE UNDER THE CUSTOMS ACT, 1962	
Section	**Description of Offence**
132	False declaration, false documents, etc.

PART C
An offence which is the offence of cross border implications and is specified in, —
(1) Part A; or
(3) the offences against property under Chapter XVII of the Indian Penal Code.
(4) The offence of the wilful attempt to evade any tax, penalty or interest referred to in section 51of the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015.

Sample Questions

1. Which of the following will be considered as a Scheduled Offence?
   a) As mentioned in Part A of the Schedule
   b) As mentioned in Part B of the Schedule
   c) As mentioned in Part C of the Schedule
   d) All of the above

2. Which of the following is a critical element, for an offence to be termed as a money laundering offence?
   a) Generation of proceeds of crime
   b) Doing an activity not included in the list of scheduled offences
   c) Commission of a scheduled offence
   d) None of the above

3. Which of the following will be considered as a money laundering offence?
   a) Contravention in relation to cannabis plant and cannabis.
   b) Contravention in relation to manufactured drugs and preparations
   c) Contravention in relation to psychotropic substances
   d) All of the above

4. Offences under Bharatiya Nyaya Sanhita (BNS) 2023 are covered under which part of scheduled offences?
   a) Part A of the Schedule.
   b) Part B of the Schedule
   c) Part C of the Schedule
   d) All of the above

Chapter-5 Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF) Guidelines

Learning Objective- After studying this chapter, you should know about:

- Background, purpose and scope of CFT and PF Guidelines along with General Obligations of Financial Service Providers (SPs).

5.1 Introduction to AML & CFT Guidelines

The Prevention of Money-Laundering Act, 2002 ('PMLA') forms the core of the legal framework put in place by India to combat Money Laundering activities. PMLA envisages certain guidelines for record-keeping and reporting obligations for financial institutions and persons carrying on designated business or profession. These guidelines shall be called AML & CFT Guidelines for Reporting Entities.[13] Persons carrying on designated business or profession are defined in Clause (s) of sub-section (1) of Section 2 of the PMLA (covered in chapter 2). Sub-clause (vi) of the said clause includes within the ambit of 'person carrying on designated business or profession' such persons who carry on activities as the Central Government may, by notification, designate from time-to-time.

The AML & CFT Guidelines for reporting entities providing services related to Virtual Digital Assets (VDA) aim to provide a summary of the provisions of the applicable anti money laundering, counter-terrorism financing and proliferation financing legislations in India, viz.

- the Prevention of Money Laundering Act, 2002 (hereinafter referred to as the "PMLA"),
- the Unlawful Activities (Prevention) Act, 1967 (hereinafter referred to as the "UAPA"),
- The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (hereinafter referred to as the "WMDA") and rules there under

5.2 The AML/CFT/PF Guidelines

5.2.1 Section 51A of Unlawful Activities (Prevention) Act 1967

Under Section 51A of Unlawful Activities (Prevention) Act 1967[14] and orders issued thereunder, it has been specified that the Central Government shall have power to:

[13] Source- https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf
[14] Source- https://www.indiacode.nic.in/bitstream/123456789/1470/1/a1967-37.pdf

- 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, or any other person engaged in or suspected to be engaged in terrorism;
- prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
- prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

5.2.2 Section 35 of Unlawful Activities (Prevention) Act 1967

Under Section 35 of the Act, the Central government may, by notification, in the Official Gazette, —

(a) add an organisation to the First Schedule
(b) add also an organisation to the First Schedule, which is identified as a terrorist organisation in a resolution adopted by the Security Council under Chapter VII of the Charter of the United Nations, to combat international terrorism;
(c) remove an organisation from the First Schedule;
(d) amend the First Schedule in some other way.

The central government shall exercise its power in respect of an organisation only if it believes that it is involved in terrorism and the central government may, by notification in the Official Gazette, add to or remove or amend the Second Schedule or Third Schedule

5.2.3 Section 12 of The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

Under Section 12 of The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, no person who is a resident in India shall, for a consideration under the terms of an actual or implied contract, knowingly facilitate the execution of any transaction which is prohibited or regulated under this Act:

Provided that a mere carriage, without knowledge, of persons, goods or technology, or provision of services, including by a public or private carrier of goods, courier, tele-communication, postal service provider or financial service provider, shall not be an offence for the purposes of this section.

Further, the AML/CFT/PF guidelines also provide their applicability and implications for the providers of services related to Virtual Digital Assets hereinafter referred to as Service Providers (SPs) and their role in applying Anti-Money Laundering, Countering the Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF) obligations.

These guidelines are intended to set out the steps that a SP shall implement to discourage and to identify any money laundering, terrorist financing or proliferation financing activities. It prescribes the procedures and obligations to be followed by the reporting entities to ensure compliance with AML/CFT/CPF guidelines. The strategy would be to use deterrence (implementation of effective KYC, CDD and EDD measures), detection (e.g., monitoring and suspicious 7 transaction reporting), and record-keeping so as to facilitate investigations by the appropriate authorities wherever required.

The term Service Provider (SP) means a person carrying out the following activities for another natural or legal person in the course of business

- 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

5.2.4 Purpose and Scope of the Guidelines

The purpose of these guidelines is to:

- Understand and apply the risk-based approach and indicate best practices in the design and implementation of an effective risk-based approach.
- Identify the entities that conduct activities or operations relating to VDAs i.e., SPs.
- Establish an efficient reporting mechanism to prevent money laundering, terrorist financing and proliferation financing.
- To assist entities engaged in or seeking to engage in VDA activities or operations to better understand their AML/CFT/CPF obligations and how they can effectively comply with the AML/CFT/CPF requirements as notified under PMLA/PMLR.

The Scope of these guidelines is vast and:

- The guidelines apply to SPs and explain how they should implement the AML/CFT/CPF obligations effectively.
- Further, the guidelines focus on VDAs that are convertible to other funds or value, including both VDAs that are convertible to other VDAs and VDAs that are convertible to fiat or that intersect with the fiat financial system.
- Central Bank issued Digital Currencies (CBDCs) are outside the scope of this guidance since they are digital representation of fiat currencies (government issued currency that is not backed by a precious metal)

These guidelines became effective from 10th March 2023.

The Financial Action Task Force (FATF) which leads global action to tackle money laundering, terrorist and proliferation financing activities, identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents/statements that are issued three times a year. The FATF's process to publicly list countries with weak AML/CFT regimes has proved effective. This statement, (previously called "Public Statement"), identifies countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation. This list is often externally referred to as the **Black list**. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the country.

Further, this statement identifies countries that are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the **grey list.**

The practical applicability of AML/CFT and PF guidelines have been dealt in detail in the next chapter.

Sample Questions

1. Under Section 51 An Unlawful Activities (Prevention) Act 1967, the central Government has powers to take what action?
   a) Freeze assets of persons engaged in or suspected to be engaged in terrorism
   b) Seize assets of persons engaged in or suspected to be engaged in terrorism
   c) Attach assets of persons engaged in or suspected to be engaged in terrorism
   d) All of the above

2. Exchange between virtual digital assets and fiat currencies is a service provided by which agency?
   a) Source Provider
   b) Service Provider
   c) Stability Provider
   d) Solution Provider

3. What amongst the following is NOT a purpose of CFT and PF Guidelines?
   a) Indicate best practices in the design and implementation of an effective risk-based approach
   b) Establish an efficient reporting mechanism to prevent money laundering
   c) To prevent entities from engaging in VDA activities
   d) To assist engaged entities to better understand their AML/CFT/CPF obligations

4. Under FATF Guideline, the countries subject to increased monitoring are included in which list?
   a) Grey List
   b) Black List
   c) Blue List
   d) None of the above

Chapter-6 SEBI Guidelines for Anti Money Laundering (AML) Standards, Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)

Learning Objective- After studying this chapter, you should know about:

- SEBI Guidelines on AML, CFT and PF and SEBI Master Circular dated June 06' 2024.

6.1 Introduction to SEBI Guidelines on AML, CFT and PF

The Prevention of Money Laundering Act, 2002 (PMLA) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) mandate every reporting entity which includes intermediaries registered under section 12 of the Securities and Exchange Board of India Act, 1992[15] (SEBI Act) and stock exchanges i.e. a stockbroker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, portfolio manager, investment adviser and any other intermediary associated with the SEBI and stock exchanges, to adhere to client account opening procedures, maintain records and report such transactions as prescribed therein to the relevant authorities.

The PML Rules, empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained. It also mandates the reporting entities to evolve an internal mechanism for detecting the transactions specified in the PML Rules and for furnishing information thereof.

Each intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time. The overriding principle is that they shall be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

Further, in case there is a variance in Client Due Diligence (CDD)/ Anti Money Laundering (AML) standards specified by SEBI and the regulators of the host country, branches/overseas subsidiaries of registered intermediaries are required to adopt the more stringent requirements

[15] https://www.sebi.gov.in/legal/acts/jan-1992/securities-and-exchange-board-of-india-act-1992-as-amended-by-the-finance-act-2021-13-of-2021-w-e-f-april-1-2021-_3.html

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 shall be required to apply appropriate additional measures to manage the Money Laundering/Terror Financing (ML/TF) risks, and inform SEBI.

Thus, it can be said that these guidelines provide understanding on the practical implications of the PMLA and set out the steps that a registered intermediary or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities. The step included are as mentioned hereunder:

6.1.1 Obligation to establish policies and procedures and its Mapping

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all registered intermediaries ensure the fulfilment of the aforementioned obligations.

Financial groups shall be required to implement group wide programmes for dealing with ML/TF, which shall be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group. The senior management of a registered intermediary shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The registered intermediaries shall:

a) Issue policies and procedures for sharing information required for the purposes of Client Due Diligence (CDD) and Money Laundering/Terrorist Financing (ML/TF) risk management and ensure its implementation;
b) Ensure that the content of these Directives is understood by all staff members;
c) Conduct audit and analysis of transactions or activities which appear unusual including receipt of such information from branches and subsidiaries of these group;
d) Regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;
e) Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;

f) Undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;
g) Have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
h) Develop staff members' awareness and vigilance to guard against ML and TF.

6.1.2 Policies and procedures to combat ML and TF shall cover:

i. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;
ii. Client acceptance policy and client due diligence measures, including requirements for proper identification;
iii. Maintenance of records;
iv. Compliance with relevant statutory and regulatory requirements;
v. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;
vi. Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front-line staff, of their responsibilities in this regard; and
vii. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

6.2 Written Anti Money Laundering Procedures

Each registered intermediary shall maintain written procedures to implement the anti-money laundering provisions as prescribed under the PMLA.[16] Such procedures shall include the following four specific parameters which are related to the overall 'Client Due Diligence Process':

a) Policy for acceptance of clients

[16] SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 June 06' 2024

b) Procedure for identifying the clients
c) Risk Management
d) Monitoring of Transactions

6.2.1 Client Due Diligence (CDD)

Client Due Diligence means screening and verification carried out on an existing/prospective client using reliable and independent sources of identification. It is the act of performing background checks and other screening on the customer to ensure that they are properly risk-assessed before being onboarded. CDD is at the heart of Anti-Money Laundering (AML) and Know Your Customer (KYC) initiatives.

The CDD shall have regard to the money laundering and terrorist financing risks and the size of the business and shall 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 registered intermediary or through national risk assessment. The CDD measures comprise the following:

a) Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;
b) Identify the client and verify the identity of the client using reliable and independent sources of identification, obtain information on the purpose and intended nature of the business relationship;
c) Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person acting on behalf of such client is so authorized and verify the identity of that person where the client is a/an:
    i. **Company**-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.
    Explanation: For the purpose of this sub-clause: "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company)
    ii. **Partnership firm**-the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of/

entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

iii. **Unincorporated association or body of individuals**- the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;
where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

iv. **Trust**- the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust, settlor, protector and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership

v. **Foreign investor**- Registered intermediaries dealing with foreign investors guided by SEBI directives[17], for the purpose of identification of beneficial ownership of the client.

The compliance of the aforementioned provision on identification of beneficial ownership is monitored by the Stock Exchanges and Depositories through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

a) Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);
b) Understand the nature of business, ownership and control structure of the client;
c) Conduct ongoing due diligence and scrutiny, i.e., perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;
d) Registered intermediaries shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data;

[17] Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 and amendments thereto

e) Registered intermediaries shall 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;
f) Every registered intermediary shall register the details of a client, in case of client being a non-profit organisation, on the **DARPAN Portal of NITI Aayog**, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later;
g) Where registered intermediary is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND;
h) No transaction or account-based relationship shall be undertaken without following the CDD procedure.

6.2.2 Policy for acceptance of clients

It is very important for the registered intermediaries to identify the types of clients that are likely to pose a higher than average risk of Money Laundering (ML) or Terror Financing (TF). Policy for acceptance of clients puts the registered intermediary in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. In a nutshell, the following safeguards are to be followed while accepting the clients.

a) No registered intermediary shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

b) Clients should be classified into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher; Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.

c) Enhanced due diligence measures should be carried out for Clients of Special Category (CSC). CSC shall include the following clients: NRI, HNI, Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations, Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations, Companies

having close family shareholdings or beneficial ownership; Politically Exposed Persons" (PEPs), Clients in high-risk countries, non-face to face clients and Clients with dubious reputation as per public information available.

d) Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

e) It must be ensured that an account is not opened where the intermediary is unable to apply appropriate CDD measures. The registered intermediary shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

f) The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. The rights and responsibilities of both the persons i.e., the agent-client registered with the intermediary, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

g) Necessary checks and balance should be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

h) The CDD process shall necessarily be revisited when there are suspicions of ML/TF[18].

6.2.3 Client Identification Procedure

Client Identification Procedure (CIP) is carried out at various stages like:

- to establish the intermediary – client relationship
- while carrying out transactions for the client
- when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data

[18] SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06' 2024

Registered intermediaries shall be in compliance with the following requirements while putting in place a CIP:

i. All registered intermediaries shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.
ii. All registered intermediaries are required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.
iii. Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
iv. The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
v. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
vi. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by SEBI from time to time, all registered intermediaries shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices. Further, the intermediary shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued there under so that the intermediary is aware of the clients on whose behalf it is dealing. Every intermediary shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies

rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to registered intermediaries (brokers, depository participants, AMCs etc.) from obtaining the minimum information/documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by registered intermediaries. This shall be strictly implemented by all registered intermediaries and non-compliance shall attract appropriate sanctions.

Registered intermediaries may rely on a third party for the purpose of –

i. Identification and verification of the identity of a client and
ii. Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. In terms of Rule 9(2) of PML Rules:

i. The registered intermediary shall immediately obtain necessary information of such client due diligence carried out by the third party;
ii. The registered intermediary shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
iii. The registered intermediary shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

iv. The third party is not based in a country or jurisdiction assessed as high risk;
v. The registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

6.2.4 Risk Management

Registered intermediaries shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, the registered intermediaries shall monitor the implementation of the controls and enhance them if necessary.

It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, the registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk based approach, the type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

It may be noted that low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

6.2.5 Risk Assessment

Registered intermediaries shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

The Stock Exchanges and registered intermediary shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries shall ensure:

a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
b. Adoption of a risk based approach to manage and mitigate the risks.

The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

6.2.6 Monitoring of Transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that it can identify deviations in transactions / activities.

The intermediary shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The intermediary may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/stock exchanges/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required.

The registered intermediaries shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

The intermediary shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the intermediary. Further, the compliance cell of the intermediary shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e., whether they are in the nature of suspicious transactions or not.

6.2.7 Suspicious Transaction Monitoring and Reporting

Registered Intermediaries shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, registered intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

i. Clients whose identity verification seems difficult or clients that appear not to cooperate;
ii. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
iii. Clients based in high-risk jurisdictions;
iv. Substantial increases in business without apparent cause;
v. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
vi. Attempted transfer of investment proceeds to apparently unrelated third parties;
vii. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

Any suspicious transaction shall be immediately notified to the Designated/Principal Officer within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that registered intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

Further, registered intermediaries shall ensure that clients of special categories (CSC) 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 enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

6.2.8 Record Management

Information to be maintained- Registered Intermediaries are required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

- the nature of the transactions;
- the amount of the transaction and the currency in which it is denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

6.2.9 Record Keeping

Registered intermediaries shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

Registered Intermediaries shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

In case of any suspected laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

i. the beneficial owner of the account;
ii. the volume of the funds flowing through the account; and
iii. For selected transactions:
    a. the origin of the funds the form in which the funds were offered or withdrawn, e.g., cheques, demand drafts etc.;
    b. the identity of the person undertaking the transaction;
    c. the destination of the funds;
    d. the form of instruction and authority.

Registered Intermediaries shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g., client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

More specifically, all the registered intermediaries shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

i. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;
ii. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency; It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.
iii. 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;
iv. all suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by the registered intermediary.

Where the registered entity does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the registered intermediary shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules.

6.2.10 Retention of Records

Registered intermediaries shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and intermediary.

As stated earlier, registered intermediaries are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed. Registered Intermediaries shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the intermediary.

6.2.11 Reporting to Financial Intelligence Unit-India

In terms of the PML Rules, registered intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit - India
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi-110001, INDIA
Telephone: 91-11-23314429, 23314459
91-11-23319793(Helpdesk)
Email:helpdesk@fiuindia.gov.in (For FINnet and general queries) ctrcell@fiuindia.gov.in (For Reporting Entity / Principal Officer registration related queries) complaints@fiuindia.gov.in

Website: http://fiuindia.gov.in

Registered intermediaries shall carefully go through all the reporting requirements (https://www.sebi.gov.in/sebi_data/commondocs/jun2024/Brochures on FIU_p.pdf) and formats that are available on the website of FIU – IND under the Section Home - FINNET 2.0 – User Manuals and Guides -Reporting Format (https://www.sebi.gov.in/sebi_data/commondocs/jun2024/Reporting_Format_p.pdf).

These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIUIND.

The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, registered intermediaries shall adhere to the following:

i. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month;
ii. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 of the PML Rules. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion;
iii. The Non Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month
iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;
v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND;
vi. No NIL reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported;
vii. "Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

viii. Every registered intermediary, its Directors, officers and all employees shall ensure that the fact of maintenance referred to in Rule 3 of PML Rules and furnishing of information to the Director is kept confidential. Provided that nothing in this rule shall inhibit sharing of information under Rule 3A of PML Rules of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

Registered Intermediaries shall not put any restrictions on operations in the accounts where an STR has been made. Registered intermediaries and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

The registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime. It is further clarified that "proceeds of crime" include property not only derived or obtained from 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. Confidentiality requirement does not inhibit information sharing among entities in the group.

The SEBI Guidelines discussed in detail in this chapter when implemented effectively, will help protect the financial system, help financial institutions understand their customers, reduce the risk of money laundering and Prevent Financial Institutions from being abused.

Sample Questions

1. To satisfy itself that the measures taken by it are adequate for effective implementation of PMLA 2002, every intermediary should carefully evaluate which of the following factors?
   a) Nature of Business
   b) Types of clients
   c) Nature of transactions
   d) All of the above

2. A natural person or persons who ultimately own, control or influence a client and/or person on whose behalf a transaction is being conducted is better known as……
   a) Beneficial Owner
   b) Legal Owner
   c) Sole Owner
   d) Individual Owner

3. State whether the statement is True or False- Transactions or account-based relationship can be undertaken without following the CDD procedure
   a) True
   b) False

4. Which of the following documents may not be retained by an investigation authority while investigating a matter?
   a) Client Identification records
   b) Account files
   c) Blank letter heads
   d) Business Correspondence

Chapter-7 SEBI Guidelines for KYC Norms in Securities Market

Learning Objective- After studying this chapter, you should know about:

- The KYC guidelines and process to be followed by every SEBI registered intermediary to obtain and verify the Proof of Identity (PoI) and Proof of Address (PoA) from the client at the time of commencement of an account-based relationship.

7.1 SEBI guidelines for KYC norms

KYC and Client Due Diligence (CDD) policies as part of KYC are the foundation of an effective Anti-Money Laundering process. The KYC process requires every SEBI registered intermediary to obtain and verify the Proof of Identity (PoI) and Proof of Address (PoA) from the client at the time of commencement of an account-based relationship.

The registered intermediaries shall not open or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified. The intermediaries shall also continue to abide by circulars issued by SEBI from time to time for prevention of money laundering.

7.1.1 Uniform KYC Format

SEBI registered intermediaries shall perform KYC in securities market through physical mode/ digital (online or app based) mode. To bring about uniformity in securities market, all SEBI registered intermediaries shall use the same KYC form and supporting documents

The account opening form (AOF) for client shall be divided into two parts.

a) Part I of the AOF shall be the KYC form which shall capture the basic details about the client. For this purpose, all registered intermediaries shall use the KYC templates provided by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) for individuals and for legal entities for capturing the KYC information. The CKYCR templates - Individual and Legal Entity provided by CERSAI is available at https://www.ckycindia.in/ckyc/?r=download.

b) Part II of the form shall obtain the additional information specific to the area of activity of the intermediary, as considered appropriate by them. The instant Master Circular deals with the provisions of Part I -KYC form.

While performing the KYC Process in Securities Market, the registered intermediaries shall abide by the following requirements/exemptions for effective implementation of Anti-Money Laundering process

7.1.2 Requirement of Permanent Account Number (PAN)

In order to strengthen the KYC norms and identify every participant in the securities market with their respective PAN thereby ensuring sound audit trail of all the transactions, PAN shall be the unique identification number for all participants transacting in the securities market, irrespective of the amount of transaction.

The registered intermediaries shall verify the PAN of their clients online at the Income Tax website without insisting on the original or copy of PAN card. As per the provisions of Income-tax Act, 1961 (Income Tax Act), the PAN allotted to a person shall become inoperative if it is not linked with Aadhaar. Since PAN is the key identification number and part of KYC requirements for all transactions in the securities market, all registered intermediaries shall ensure valid PAN in the KYC documentation for all clients. Status of Aadhaar and PAN linkage shall be flagged at the system of KRA.

7.1.3 Exemptions/Clarifications to PAN requirements

The following are exempted from the mandatory requirement of PAN:

i. Transactions undertaken on behalf of Central Government and/or State Government and by officials appointed by Courts e.g., Official liquidator, Court receiver etc. (under the category of Government) for transacting in the securities market.
ii. Investors residing in the state of Sikkim.
iii. UN entities/multilateral agencies exempt from paying taxes/filing tax returns in India.
iv. SIP of Mutual Funds up to ₹50,000/- per year.

In case there is change in the name subsequent to issuance of PAN of the client, registered intermediaries can collect the PAN card proof as submitted by the client provided it is supported by a marriage certificate issued by the State Government or gazette notification, indicating such a change of name. The e-PAN issued by Central Board of Direct Taxes (CBDT) can also be produced by client for KYC compliance. e-PAN is a digitally signed PAN card issued in electronic format by the Income-tax department.

7.1.4 Proof of Identity (PoI)- List of documents admissible

Registered intermediaries at the time of commencement of an account based relationship shall identify their clients, verify their identity and obtain information on the purpose and intended nature of the business relationship. The name as mentioned in the KYC form shall match the name as mentioned in the Proof of Identity (PoI) submitted. The following documents shall be accepted as PoI

a. Officially valid document (OVD) defined as per Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules):

   i. the passport;
   ii. the driving licence;
   iii. proof of possession of Aadhaar number;
   iv. the Voter's Identity Card issued by Election Commission of India;
   v. job card issued by NREGA duly signed by an officer of the State Government;
   vi. the letter issued by the National Population Register containing details of name address; or
   vii. any other document as notified by the Central Government in consultation with the Regulator.

b. Further, in terms of proviso to the above Rule, where simplified measures are applied for verifying the identity of the clients, the following documents shall also be deemed to be officially valid document:
   i. Identity card/ document with applicant's photo, issued by the Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks and Public Financial Institutions;
   ii. Letter issued by a gazetted officer, with a duly attested photograph of the person.

7.1.5 Proof of Address (PoA)- List of documents admissible

The following documents shall be accepted as PoA:

a. "officially valid document" defined as per Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules):

   i. the passport;
   ii. the driving licence;

iii. proof of possession of Aadhaar number;
iv. the Voter's Identity Card issued by Election Commission of India;
v. job card issued by NREGA duly signed by an officer of the State Government;
vi. the letter issued by the National Population Register containing details of name, address; or
vii. any other document as notified by the Central Government in consultation with the Regulator.

b. Further, in terms of Rule 9(18) of PML rules, 2005, in case the officially valid document furnished by the client does not contain updated address, the following documents (or their equivalent e-documents thereof) shall be as deemed to be officially valid document for the limited purpose of proof of address, provided that the client shall submit updated officially valid document (or their equivalent e-documents thereof) with current address within a period of three months of submitting the following documents:

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. letter of allotment of accommodation from employer issued by state or central government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

In terms of the PML Rules, cases where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as is issued by the UIDAI. A document shall be deemed to an officially valid document even if there is a change in the name subsequent to its issuance provided it is supported by a Marriage Certificate issued by the State Government or a gazette notification, indicating such change of name.

For non-residents and foreign nationals, (allowed to trade subject to RBI and FEMA guidelines), copy of passport/Persons of Indian Origin (PIO) Card/Overseas Citizenship of India (OCI) Card and overseas address proof is mandatory. In case the officially valid document presented by a foreign national does not contain the details of address, the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. If any proof of address is in a foreign

language, then translation into English shall be required. If correspondence and permanent address is different, then proof for both shall be submitted.

7.1.6 Acceptance of third party address as correspondence add

Registered intermediaries at the time of commencement of an account based relationship shall determine whether the client purports to act on behalf of juridical person or individual or trust and the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

A client can authorize to capture address of a third party as a correspondence address, provided that all prescribed 'Know Your Client' norms are also fulfilled for the third party. The intermediary shall obtain proof of identity and proof of address for the third party. The intermediary shall also ensure that client due diligence norms as specified in Rule 9 of PML Rules are complied with in respect of the third party.

7.1.7 Identification of Beneficial Ownership

SEBI Master Circular SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06, 2024 on Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under has prescribed the approach to be followed towards identification of beneficial ownership. Accordingly, the registered intermediaries may be guided by the provisions of the said Master Circular and amendments thereto for the purpose of identification of beneficial ownership of the client.

Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures.

The registered intermediaries shall conduct ongoing CDD where inconsistencies are noticed in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, PML Rules, SEBI Act and Regulations, directives and circulars issued thereunder so that the intermediary is aware of the clients on whose behalf it is dealing. The registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

The stock exchanges and depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of

mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

7.1.8 Requirement of additional documents for non-individuals (Legal Entities)

In case of non-individuals, additional documents (certified copies of equivalent e-documents) to be obtained are mentioned below:

i. Corporate body:

a. Certificate of incorporation
b. Memorandum and Articles of Association.
c. Board Resolution for investment in securities market.
d. Power of Attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf.
e. Authorised signatories list with specimen signatures.
f. Copy of the balance sheet for the last financial year (initially for the last two financial years and subsequently for every last financial year).
g. Latest share holding pattern including list of all those holding control, either directly or indirectly, in the company in terms of SEBI takeover Regulations, duly certified by the company secretary/whole time director/ MD (to be submitted every year).
h. Photograph, POI, POA, PAN and DIN numbers of whole-time directors/two directors in charge of day to day operations.
i. Photograph, POI, POA, PAN of individual promoters holding control - either directly or indirectly.

ii. Partnership firm:

a. Certificate of registration (for registered partnership firms only).
b. Copy of partnership deed.
c. Copy of the balance sheet for the last financial year (initially for the last two financial years and subsequently for every last financial year).
d. Authorised signatories list with specimen signatures.
e. Photograph, POI, POA, PAN of Partners.

iii. Trust:

a. Certificate of registration (for registered trust only).

b. Copy of Trust deed.
c. Copy of the balance sheet for the last financial year (initially for the last two financial years and subsequently for every last financial year).
d. List of trustees certified by managing trustees/CA.
e. Photograph, POI, POA, PAN of Trustees.

iv. HUF:

a. Deed of declaration of HUF/ List of coparceners.
b. Bank pass-book/bank statement in the name of HUF.
c. Photograph, POI, POA, PAN of Karta.

v. Unincorporated association or a body of individuals:

a. Proof of Existence/Constitution document.
b. Resolution of the managing body & Power of Attorney granted to transact business on its behalf.
c. Authorized signatories list with specimen signatures.

vi. Banks/Institutional Investors:

a. Copy of the constitution/registration or annual report/balance sheet for last financial year (initially for the last two financial years and subsequently for every last financial year).
b. Authorized signatories list with specimen signatures.

vii. Army/ Government Bodies:

a. Self-certification on letterhead.
b. Authorized signatories list with specimen signatures.

viii. Registered Society:

a. Copy of Registration Certificate under Societies Registration Act.
b. List of Managing Committee members.
c. Committee resolution for persons authorised to act as authorised signatories with specimen signatures.
d. True copy of Society Rules and Bye Laws certified by the Chairman/Secretary.

7.1.9 Requirement of Mobile Number and Email ID

The registered intermediaries shall upload the details of mobile number and email address on the KRA system. It shall be ensured that the mobile number/email addresses of their employees/authorized persons, distributors etc. are not uploaded on behalf of clients.

7.1.10 Digital KYC

In order to enable the online KYC process for establishing account-based relationship with the registered intermediary, client's KYC shall be completed through digital (online / Application (App) based) KYC, in person verification through video, online submission of officially valid document / other documents, using electronic/digital signature, including Aadhaar e-Sign.

i. The client shall visit the website/App/digital platform of the registered intermediary and fill up the online KYC form and submit requisite documents.
ii. SEBI registered intermediaries shall obtain the express consent of the client before undertaking online KYC.
iii. The PAN, name, photograph, address, mobile number and email ID of the client shall be captured digitally and officially valid document shall be provided as a photo / scan of the original under electronic/digital signature, including Aadhaar e-Sign and the same shall be verified.
iv. Any officially valid document other than Aadhaar shall be submitted through Digiocker / using electronic/digital signature, including Aadhaar eSign.
v. The mobile number of client accepted as part of KYC should preferably be the one seeded with Aadhaar.
vi. Mobile and email shall be verified through One Time Password (OTP) or other verifiable mechanism.
vii. Aadhaar shall be verified through UIDAI's authentication/ verification mechanism. Further, in terms of PML Rule 9(16), every intermediary shall, where the client submits his Aadhaar number, ensure that such client redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15) under PML Rule.
viii. e-KYC through Aadhaar Authentication service of UIDAI (e-KYC) or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar Secure QR Code generation date is not older than 3 days from the date of carrying out KYC.
ix. The usage of Aadhaar shall be optional and purely on a voluntary basis by the client.

x. Any document, except for the documents mentioned in the First Schedule of the Information Technology Act, 2000, shall be authenticated by a client by way of electronic/digital signature including Aadhaar e-Sign. Accordingly, the process of performing KYC shall be completed by using electronic/digital signature including Aadhaar e-Sign.

xi. A client can use the electronic/digital signature, including Aadhaar e-Sign service to submit the document to the registered intermediary.

xii. In case of non-individual clients, intermediaries shall exercise caution and satisfy themselves regarding the genuineness of the authorization and identity of the authorized signatories.

xiii. The electronic/digital signature, including Aadhaar e-Sign shall be accepted in lieu of wet signature on the documents provided by the client. The cropped signature affixed on the online KYC form under electronic/digital signature, including Aadhaar e-Sign shall also be accepted as valid signature.

xiv. Bank details of the client shall be captured online and signed cancelled cheque shall be provided as a photo / scan of the original under electronic/digital signature including Aadhaar e-Sign. Bank account details shall be verified by Penny Drop mechanism or any other mechanism using API of the Bank. The name and bank details as obtained shall be verified with the information provided by client.

xv. Once all the required information as per the online KYC form is filled up by the investor, KYC process shall be completed as under:

    a. The client shall take a print out of the completed KYC form and after affixing their wet signature, send the scanned copy / photograph of the same to the registered intermediary under electronic/digital signature including Aadhaar e-Sign or

    b. Affix online the cropped signature on the filled KYC form and submit the same to the registered intermediary under electronic/digital signature including Aadhaar e-Sign.

    c. The “original seen and verified” requirement for officially valid document would be met where the investor provides the officially valid document in the following manner:

        i. As a clear photograph or scanned copy of the original officially valid document, through the electronic/digital signature including Aadhaar e-Sign, or

        ii. As digitally signed document of the officially valid document, issued through the DigiLocker by the issuing authority.

Further, in order to ensure accessibility and inclusiveness of Digital KYC to persons with disabilities, SEBI has issued guidelines for intermediaries.[19]

7.2 Features for online KYC App of the Intermediary

SEBI registered intermediary can implement its own App for undertaking online KYC of clients. The App shall facilitate taking photograph, scanning, acceptance of officially valid document through Digilocker, video capturing in live environment and usage of the App only by authorized person of the intermediary.

The App shall also have features of random action initiation for client response to establish that the interactions are not pre-recorded along with time stamping and geo-location tagging to ensure the requirement like physical location being in India etc. are also implemented. Registered intermediaries shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the client and the quality of the communication is adequate to allow identification of the client beyond doubt. Registered intermediaries shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations. The intermediaries shall, before rolling out and periodically, carry out software and security audit and validation of their App. The intermediaries can have additional safety and security features other than as prescribed above.

7.2.1 Requirement of In-Person Verification (IPV)

It shall be mandatory for all the registered intermediaries to carry out IPV of their clients. The intermediaries shall ensure that the details like name of the person doing IPV, his designation, organization with his signatures and date are recorded on the KYC form at the time of IPV. The IPV carried out by one SEBI registered intermediary can be relied upon by another intermediary.

In case of Stock brokers, their Authorised Persons (appointed by the stock brokers after getting approval from the concerned Stock Exchanges) can perform the IPV. In case of Mutual Funds, their Asset Management Companies (AMCs) and the distributors who comply with the certification process of National Institute of Securities Market (NISM) or Association of Mutual Funds (AMFI) and have undergone the process of 'Know Your Distributor (KYD)', can perform the IPV. Additionally, entities registered as Category 1 Execution Only Platform (EOP) can perform the IPV. In case of applications received by the mutual funds directly from the clients

[19] https://www.sebi.gov.in/legal/circulars/may-2025/accessibility-and-inclusiveness-of-digital-kyc-to-persons-with-disabilities_94096.html

(i.e., not through any distributor), they may also rely upon the IPV performed by the scheduled commercial banks.

To enable ease of completing IPV of an investor, intermediary may undertake the Video in Person Verification (VIPV) of an individual investor through their App. The following process shall be adopted in this regard:

a) Intermediary through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual client, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.
b) The VIPV shall be in a live environment.
c) The VIPV shall be clear and still, the client in the video shall be easily recognisable and shall not be covering their face in any manner.
d) The VIPV process shall include random question and response from the investor including displaying the officially valid document, KYC form and signature or could also be confirmed by an OTP.
e) The intermediary shall ensure that photograph of the client downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.
f) The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.
g) The intermediary may have additional safety and security features other than as prescribed above.

IPV shall not be required in the cases where:

a) the KYC of the client has been completed using the Aadhaar authentication/ verification of UIDAI.
b) the KYC form has been submitted online, documents have been provided through Digilocker or any other source which could be verified online.

7.2.2 Adaptation of Aadhaar based e-KYC process and e-KYC Authentication facility for Resident Investors under section 11A of the Prevention of Money Laundering Act, 2002: KUA and Sub KUA mechanism

Registered intermediaries for reasons such as online on-boarding of clients, client convenience, increased efficiency and reduced time for client onboarding would prefer to use Aadhaar based e-KYC facility to complete KYC of the client. The e-KYC service

launched by UIDAI shall be accepted as a valid process for KYC verification. As per the process outlined by Department of Revenue (DoR), Ministry of Finance (MoF) vide circular dated May 09, 2019 for use of Aadhaar authentication services by entities in the securities market as may be notified by the Central Government shall be allowed to undertake Aadhaar Authentication under section 11A of the PMLA .These entities would be registered with UIDAI as KYC user agency (KUA)/sub KYC user Agency (sub-KUA).The KUAs shall allow the SEBI registered intermediaries as sub-KUA to undertake Aadhaar Authentication of their clients for the purpose of KYC.

The following entities shall get registered with UIDAI as KYC user agency ("KUA") and shall allow SEBI registered intermediaries to undertake Aadhaar Authentication in respect of their clients for the purpose of KYC.

(i) Bombay Stock Exchange Limited
(ii) National Securities Depository Limited
(iii) Central Depository Services (India) Limited
(iv) CDSL Ventures Limited
(v) NSDL Database Management Limited
(vi) NSE Data and Analytics Limited
(vii) CAMS Investor Services Private Limited
(viii) Computer Age Management Services Private Limited
(ix) National Stock Exchange of India Limited (NSE).

SEBI registered intermediaries who want to undertake Aadhaar authentication services through KUAs, shall enter into an agreement with any one KUA and get themselves registered with UIDAI as Sub-KUAs. The agreement in this regard shall be as prescribed by UIDAI.

7.3 KYC for SARAL Account Opening Form for resident individuals

For individual clients participating in the cash segment without obtaining various other facilities such as internet trading, margin trading, derivative trading and use of power of attorney, the requirement of submission of 'proof of address' shall be as follows:

a. Individual client may submit only one documentary proof of address (either residence/correspondence or permanent) while opening a trading account and / or demat account or while undergoing updation.
b. In case the proof of address furnished by the said client is not the address where the client is currently residing, the intermediary may take a declaration of the

residence/correspondence address on which all correspondence shall be made by the intermediary with the client. No proof is required to be submitted for such correspondence/residence address. In the event of change in this address due to relocation or any other reason, client may intimate the new address for correspondence to the intermediary within two weeks of such a change. The residence/ correspondence address and any such change thereof may be verified by the intermediary through 'positive confirmation' such as:

i. acknowledgment of receipt Welcome Kit/ dispatch of contract notes / any periodical statement, etc.
ii. telephonic conversation;
iii. visits, etc.

c. The registered intermediaries shall forward the KYC completion intimation letter through registered post/ speed post or courier, to the address of the client in cases where the client has given address other than as given in the officially valid document. In such cases of return of the intimation letter for wrong / incorrect address, addressee not available etc., no transactions shall be allowed in such account and intimation shall also sent to the Stock Exchange and Depository.
d. The registered intermediaries and KRAs shall flag such accounts in their records/systems.

7.3.1 Confidentiality of client information

Registered intermediaries shall keep confidential every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force.

7.4 Know Your Client (KYC) Registration Agency

A mechanism of Know Your Client Registration Agency (KRAs) in the securities market has been developed for centralization of the KYC records. The KRAs shall be administered under SEBI KYC Registration Agency (KRA) Regulations, 2011.

7.5 Guidelines for Intermediaries

The client shall be allowed to open an account with intermediaries and transact in securities market as soon as the KYC process is completed. After doing the initial KYC of the new clients, the intermediary shall forthwith upload the KYC information on the system of the KRA within 3 working days from the date of completion of KYC process. In case a client's KYC documents sent by the intermediary to KRA are not complete, the KRA shall inform the same to the intermediary who shall forward the required information / documents promptly to KRA. For

existing clients, the KYC data shall be uploaded by the intermediary provided they are in conformity with details sought in the uniform KYC format. While uploading these clients' data the intermediary shall ensure that there is no duplication of data in the KRA system. The intermediaries shall maintain electronic records of KYCs of clients and keeping physical records would not be necessary. The intermediary shall promptly provide KYC related information to KRA, as and when required. The intermediary shall have adequate internal controls to ensure the security / authenticity of data uploaded by it.

7.5.1 Guidelines for KRAs

KRA system shall provide KYC information in data and image form to the intermediary. KRA shall send a letter to the client within 2 working days of the receipt of the initial/updated KYC documents from intermediary, confirming the details thereof and maintain the proof of dispatch. KRA(s) shall develop systems, in co-ordination with each other, to prevent duplication of entry of KYC details of a client and to ensure uniformity in formats of uploading / modification / downloading of KYC data by the intermediary. KRA shall maintain an audit trail of the upload / modifications / downloads made in the KYC data, by the intermediary in its system. KRA shall ensure that a comprehensive audit of its systems, controls, procedures, safeguards and security of information and documents is carried out annually by an independent auditor. The Audit Report along with the steps taken to rectify the deficiencies, if any, shall be placed before its Board of Directors. Thereafter, the KRA shall send the Action Taken Report to SEBI within 3 months. KRA systems shall clearly indicate the status of clients falling under PAN exempt categories viz. investors residing in the state of Sikkim, UN entities / multilateral agencies exempt from paying taxes / filing tax returns in India, etc.

With effective implementation of SEBI guidelines for KYC norms in Securities Market by market intermediaries, SEBI's crucial role in maintaining market integrity, investor confidence, and the orderly functioning of India's financial markets can be duly and efficiently achieved.

Sample Questions

1. For the purpose of Client Due Diligence, the KYC process requires every SEBI registered intermediary to obtain and verify which of the following documents from the clients?
   a) Proof of Identity
   b) Proof of Address
   c) Any one of the above
   d) Both a & b

2. Q2- Which of the following shall be the unique identification number for all participants transacting in the securities market, irrespective of the amount of transaction?
   a) PAN
   b) Email id
   c) Mobile No.
   d) Correspondence Address

3. Transactions undertaken on behalf of Central Government and/or State Government and by officials appointed by Courts are exempted from the mandatory requirement of PAN. State whether True or False
   a) True
   b) False

4. In case of non-individual clients, which of the following is NOT a mandatory document to be obtained from them?
   a) Certificate of incorporation
   b) Memorandum and Articles of Association
   c) Authorised signatories list with specimen signatures
   d) Future trade plan of the client

Chapter-8 Discussion on PMLA related Cases

Learning Objective: After studying this chapter, you should know about:

- Practical implementation and coverage of PMLA through case studies.

This Chapter covers different cases based on SEBI Adjudicating Orders in the scope of Prevention of Money Laundering Act (PMLA). They are described in the following manner.

8.1 FIU-IND V/S Way2Wealth Brokers Private Limited

Summary of Order-in-Original No. 29/DIR/FIU-IND/2022 dated 10.11.2022 in the matter of Way2Wealth Brokers Private Limited (Reporting Entity) – reg.

As part of its supervisory functions under Prevention of Money Laundering Act (PMLA), Financial Intelligence Unit-India (FIU-IND) takes up cases where apparent or potential non-compliances of relevant obligations have been observed. They are carried out with a view towards identifying weaknesses in the safeguards implemented by 'reporting entities' and for conducting enforcement activity where non-compliances are found. In relation to the securities market such actions are taken to ensure that all possible safeguards, as required by law, were effectively implemented by the reporting entities so as to ensure malicious actors do not take advantage of the capital flows therein. In this regard, FIU-IND works closely with various sectoral regulators including, the Securities and Exchange Board of India (SEBI).

Facts of the case

Based on a reference from the SEBI highlighting alleged non-compliance with PMLA guidelines by Way2Wealth Brokers Private Limited, FIU-IND had taken up the case for further analysis in order to examine whether there was any non-compliance by the reporting entity with respect to the obligations under Chapter IV of PMLA.

After examining the material on record and the submissions made, Way2Wealth Brokers Private Limited was found to have breached the relevant obligations in respect of:

- its underlying transactions in December 2021. Failure of the reporting entity to properly raise, investigate alerts, handle the alerts and to file the same as a Suspicious Transaction Report (STR) with FIU-IND;

- failure of the reporting entity to properly raise an alert and consider adverse orders of SEBI from the perspective of AML transactional monitoring and reporting obligations.

Findings of the Case & Order

- In view of the facts and due to the deficiencies observed in the mechanism implemented by the reporting entity, it was found appropriate to issue monetary penalty of Rs. 1 Lac under section 13(2)(d) to Way2Wealth Brokers Private Limited along with detailed directions to the reporting entity under section 13(2)(a) and 13(2)(b).
- Way2Wealth Brokers Private Limited was further required to return, within a period of 30 days, a certification under signature of its Designated Director and Principal Officer that the directed measures would be implemented within the periods prescribed.

8.2 SEBI V/S SKSE Securities Limited

Facts of the case

SEBI conducted inspection into the books of account and other records of SKSE Securities Limited (notice) to examine its Anti Money Laundering (AML) mechanism and compliance level.

On the basis of findings of the inspection:

- It was alleged in the show cause notice that the Noticee had not implemented AML mechanism.
- It was also alleged in the Show Cause Notice (SCN) that the Noticee had not categorised the clients into high, medium and low category and hence was not exercising additional due diligence for monitoring the transactions of high and medium risk clients as compared to low risk clients.
- It was further alleged in the SCN that the Noticee had not appointed the 'Principal Officer' as required under the SEBI circular in time and even after appointment of the 'Principal Officer', the details of the 'Principal Officer' were intimated to FIU with a delay. It was thus alleged that the Noticee has violated the regulatory provisions.

Findings of the Case

- SEBI vide its Circular No. ISD/CIR/RR/AML/1/06 dated January 18, 2006 issued guidelines on AML standards and advised all intermediaries to ensure that a proper policy framework as per the guidelines on anti-money laundering measure is put into place within one month

from the date of the circular. In the instant case, the Noticee has failed to implement the said policy in time.

- Guidelines on AML standards were issued by SEBI vide its Circular dated January 18, 2006 to all SEBI registered intermediaries which required the intermediaries to develop customer acceptance policies and procedures aimed at identifying the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. In terms of the said SEBI Circular, the Noticee being SEBI registered intermediary, was clearly under obligation to implement the same. This, in turn would enable them to apply customer due diligence on a risk sensitive basis depending upon the type customer business relationship. Certain safeguards were also prescribed to be followed while accepting the clients which required classification into low, medium and high risk. This ought to have been implemented by the Noticee within one month from January 18, 2006 being the date of issuance of the Circular. It was evident from the reply of the Noticee that it had not taken any steps towards implementation till 2010. It was also noted that the categorization of old clients was still being carried on by the Noticee even then. Thus, it was noted that the Noticee had violated the provisions of SEBI Circular in this regard

- The aforementioned SEBI Circular dated January 18, 2006 mandates that the intermediaries designate an officer as 'Principal Officer' who would be responsible for ensuring the compliance of the provisions of the Prevention of Money Laundering Act, 2002 (PMLA). The name, designation and addresses (including e-mail address) of the 'Principal Officer' had to be intimated to the Office of the Director, FIU on an urgent basis. In the instant case, the appointment of 'Principal Officer' was made by the Noticee on December 14, 2007, i.e., with a delay of almost two years from the date of the SEBI Circular. Further, the appointment was also not intimated to the Director- FIU on an urgent basis. It was intimated only on January 10, 2008. Hence, it was found that the Noticee had not complied with the provisions of SEBI Circular in time.

Order

SEBI imposed a penalty of Rs. 2,00,000/- (Rupees Two Lakhs only) on the Noticee in terms of section 15HB of the SEBI Act. The above-mentioned penalty was found to be commensurate with the violation committed by the Noticee.

8.3 SEBI V/S Raima Equities Private Limited

Facts of the Case

Securities and Exchange Board of India (SEBI) had conducted an inspection of the books of accounts and other records of Raima Equities Private Limited (Noticee), a stock broker registered with SEBI for the period from April 2011 till July 02, 2012 to verify whether the Noticee is complying with the provisions of Anti Money Laundering (AML) or not.

- It was observed that the Noticee had no basis while classifying clients into high, medium and low risk.
- The Noticee had no system in place to monitor transactions from the view point of "Anti Money Laundering and Combating Financing of Terrorism". The entire concept of risk management system of the Noticee was limited to stock market risks i.e., delivery, payment, margin, etc.
- The Noticee had not even set any parameters in its system which could generate suspicious transaction reports (STRs). STRs received from depository had been closed by the Principal Officer of the Noticee without stipulating any reason in writing.
- The Noticee had no system in place to identify whether a client or potential client was a Politically Exposed Person (PEP) or not.

Findings of the Case

- The Assessing Officer (AO) did not find any merit in the submission of the Noticee that all the clients are categorized by the Noticee under 'low', medium' and 'high' risk not only on the basis of their income but also their financial credibility (wealth), relations or introducers, margin held and past performance regarding payment. No documentary evidence showing the networth of clients being good during the relevant period under inspection had been produced by the Noticee in support of its contention. Thus, the AO found that categorizing certain client under the 'low' risk category is indeed arbitrary on the part of the Noticee.

- The AO did not find any merit in the submissions of the Noticee that the STRs generated or received from the DP or the stock exchanges were properly analyzed as per the PMLA policy and no documentary evidence had been submitted by the Noticee to show as to how the STRs are dealt with by the Principal Officer. From the submissions of the Noticee, it was concluded that there does not seem to be any internal policy / system to deal with the STRs and that the STRs were being closed by the Principal Officer without giving any reasons in writing.

- With respect to allegation of no system in place to identify whether a client is a PEP or not, the Noticee had submitted that the clients are introduced by the directors / shareholders or the sub brokers of the company and thus, they all are known persons. The AO did not find any merit in the said submission and the same clearly indicates that the Noticee does not have any system in place to identify the PEP.

Order

The AO imposed a monetary penalty of Rs. 2,00,000/- (Rupees Two Lakh Only) under Section 15HB of the SEBI Act, 1992 on Raima Equities Private Limited

8.4 SEBI vs Marfatia Stock Broking Private Limited

SEBI conducted an inspection of books of accounts, documents and other records of Marfatia Stock Broking Private Limited (Marfatia) for the period from April 1, 2012 to March 31, 2013 to ascertain whether the Anti-Money Laundering (AML) Policy was in place within 30 days of the promulgation of SEBI circular ISD/CIR/RR/AML/1/06 dated January 18, 2006 read with SEBI Master Circular No. CIR/ISD/AML/3/2010 dated December 31, 2010 on Anti Money Laundering and whether there is a violation of Clause A(1), A(2) and A(5) of Code of Conduct specified under Schedule II read with Regulation 9 of SEBI (Stock Broker) Regulations, 1992 (hereinafter referred to as Brokers Regulations) and regulation 26(xvi) of Brokers Regulations.

In this regard, a show-cause notice was issued to the Marfatia. In response, Marfatia submitted their reply through letter and was granted an opportunity of personal hearing before the Adjudicating Officer. The following issues were considered:

(a) Whether Marfatia has violated the provisions of Circular No. ISD/CIR/RR/AML/1/06 dated January 18, 2006 read with SEBI Master Circular No. CIR/ISD/AML/3/2010 dated December 31, 2010; Clause A (1), A (2) and A (5) of Code of Conduct specified under Schedule II read with Regulation 9 of Brokers Regulations and regulation 26(xvi) of Brokers Regulations?

(b) Do the violations, if any, on the part of Marfatia attract monetary penalty under section 15HB of SEBI Act?

(c) If so, what would be the quantum of monetary penalty that can be imposed on Marfatia after taking into consideration the factors mentioned in section 15J of the SEBI Act read with the Adjudication Rules?

Findings of the case

As per the Circular No. ISD/CIR/RR/AML/1/06 dated January 18, 2006, Marfatia was required to have an AML policy in place within 30 days from the date of the said Circular. Marfatia had admitted that it had adopted AML policy on June 30, 2009. However, it had submitted that though a separate AML Policy was not documented, but the requirements of PMLA were duly incorporated in the relevant policies itself like KYC policy and RMS policy. The purpose of having the documented procedure is to ensure compliance with the regulatory requirements and maintain internal controls to put checks and balances to curb money laundering by incorporating various requirements. It is noted that Marfatia had documented processes for activities like the Client Registration process and risk management control although there was no separate documented policy within the prescribed timeline, the various requirements were adopted in other policies. In view of the same, the allegation of not complying with the provisions of the circular does not stand established.

With regard to the appointment of Principal Officer, when the inspection team had sought the comments of Marfatia regarding the appointment of Principal Officer, it had submitted that Mr. Vijaykumar Bharatbhai Shah was appointed on March 19, 2008. During the adjudication proceedings, Marfatia submitted a copy of letter dated February 13, 2006 addressed to the FIU mentioning that it had appointed Mr. Hiren Bipin Chandra Shah as a Principal Officer on February 2, 2006. The copy of the said letter was never brought to the notice of SEBI before the adjudication proceedings. Also, Marfatia had submitted only the proof of despatch of the said letter in the form of a courier slip of a courier company and there is no proof of delivery. Since there is nothing on record to suggest the contrary, Adjudicating Officer was inclined to accept the submission of Marfatia that it had appointed Mr. Hiren Bipin Chandra Shah as the Principal Officer on February 02, 2006 and has duly informed FIU about it. Hence, there is no violation on the part of the Marfatia.

Order

The observations made during the inspection were procedural in nature and all of these were complied with after being pointed out by the inspection team. No serious observations were made where the investors' interests would have been adversely affected. The Adjudicating Officer did not find the case fit for imposing monetary penalty and disposed of the Marfatia of the Show Cause Notice.

8.5 SEBI vs. Shreepati Holdings & Finance Pvt. Ltd.

SEBI carried out an inspection of books of accounts, documents and other records of Shreepati Holdings & Finance Pvt., Ltd., Stock Broker (SHF) on February 13 and 18, 2015, inter alia, to examine the systems put in place by SHF to comply with the Anti-Money Laundering (AML) and Combating the financing of terrorism (CFT) norms. The period of inspection was Financial Year 2013-14 and April 1, 2014 till December 31, 2014 ("inspection period"). Pursuant to the communication of findings of inspection to the SHF and analysing its' reply therein, SEBI initiated Adjudication proceedings against the SHF for the alleged violation of SEBI Circulars ref. no. (a) CIR/ISD/AML/3/2010 dated December 31, 2010, (b) CIR/MIRSD/2/2013 dated January 24, 2013, (c) CIR/MIRSD/11/2014 dated March 12, 2014, Clauses A (2) and A (5) of the Code of Conduct read with Regulation 9 (f), Regulations 26 (xv), (xvi) and (xx) of SEBI (Stock Brokers) Regulations, 1992 (hereinafter referred to as Stock Brokers Regulations).

Issues for consideration

a. Whether SHF has violated the provisions of SEBI Circulars ref. no. (a) CIR/ISD/AML/3/2010 dated December 31, 2010, (b) CIR/MIRSD/2/2013 dated January 24, 2013, (c) CIR/MIRSD/11/2014 dated March 12, 2014, Clauses A (2) and A (5) of the Code of Conduct read with Regulation 9 (f), Regulations 26 (xv), (xvi) and (xx) of SEBI (Stock Brokers) Regulations, 1992 (hereinafter referred to as Stock Brokers Regulations).

b. Does the violation, if any, attract monetary penalty under Section 15HB of SEBI Act?

c. If so, what would be the monetary penalty that can be imposed taking into consideration the factors mentioned in Section 15J of SEBI Act?

Allegations and findings

1. SHF had delayed in updating the AML Policy, in terms of SEBI Circular dated March 12, 2014. SHF in its reply to the SCN admitted that it had updated the AML Policy on November 23, 2014, which resulted in a delay of 8 months. SHF also argued that the SEBI Circular dated March 12, 2014 did not prescribe any fixed timeline within which an intermediary was required to update the AML policy. The argument did not find merit, as SHF cannot absolve it from the mandatory obligation of immediate compliance of the provisions of the SEBI Circular. Therefore, it was found that SHF did not comply with the provisions of the SEBI Circular dated March 12, 2014.

2. During the inspection period, as per the manual transaction reviewing system, SHF had submitted that no suspicious alerts have been generated by it. However, during the said period, SHF had received suspicious transaction alerts from National Stock Exchange (NSE) and Bombay Stock Exchange (BSE). As per the Stock Exchange circular requirements, SHF was required to analyse those alerts, update Know Your Customer (KYC) information of the concerned clients, where required, seek an explanation from the clients involved, seek additional documentary evidence, etc., and then record the final observations after the analysis.

3. SHF had received 83 alerts from BSE and 54 alerts from NSE during the period of inspection. It was observed in the inspection that SHF closed all the alerts received from the exchanges without assigning any reason for the same and did not maintain any record, either electronic or written, of the reasons for closing those alerts. There were no records available, either electronic or written, of the data which were examined while closing those alerts. No additional information or documents were sought from the involved clients in order to analyse the alerts.

4. SHF did not have any system/ mechanism to monitor transactions with respect to client transactions vis-à-vis the declared client financials. It was corroborated by the fact that the SHF did not have any written down policy on such alerts and also did not generate any alerts during the period under consideration.

Conclusions

1. SHF had violated the provisions of SEBI Circulars dated December 31, 2010, January 24, 2013 and March 21, 2014, Clauses A (2) and A (5) of the Code of Conduct read with Regulation 9 (f), Regulations 26 (xv), (xvi) and (xx) of SEBI (Stock Brokers) Regulations.

2. SHF had admittedly not rectified the observations made in the inspection. SHF took corrective steps only after issuance of Show Cause Notice (SCN) in the instant proceedings. It was noted that the non-compliance with SEBI's directions issued to give effect to the amendments carried out to PMLA and PML Rules, in order to prevent money laundering and terror financing, was grave in nature.

3. SHF had not taken steps to rectify the deficiencies observed in the inspection immediately after the same were brought to its' notice, but rectified in the month of February 2015 only after issuance of SCN in the instant proceedings in August, 2017 i.e., after a delay of more

than two years. Had the inspection been not carried out and the instant proceedings have not been carried out, SHF would have remained non-compliant with respect to AML & CFT.

4. The Directives issued by SEBI from time to time set out the steps that a registered intermediary or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities. Any lapse in non-compliance of the same by an Intermediary poses a serious threat to the national economy and national interest. Therefore, there is a need to impose a penalty on SHF which will act as a deterrent in future.

Order

A penalty of Rs. 3,00,000/- (Rupees Three lakhs only) was imposed on, Shreepati Holdings & Finance Pvt., Ltd., under Section 15HB of SEBI Act for violation of the provisions of SEBI Circulars dated December 31, 2010, January 24, 2013 and March 21, 2014, Clauses A (2) and A (5) of the Code of Conduct read with Regulation 9 (f), Regulations 26 (xv), (xvi) and (xx) of SEBI (Stock Brokers) Regulations, which was commensurate with the violations.[20]

The above cases direct securities market entities to adhere to regulatory directives and meet compliances so as to safeguard market integrity, protect investors' confidence and protect reputation of the market players.

8.6 BOI Shareholding Limited (BOISL) v/s SEBI

SEBI, on June 29, 2015 conducted an inspection of the appellant's (BOISL) books of accounts to examine whether the appellant had put in place systems and processes to comply with the Circulars issued by SEBI relating to the AML policy to be adopted, among others. The appellant was asked to explain the discrepancies noticed vide SEBI's letter dated July 2, 2015. The appellant replied on November 16, 2015 stating that all the discrepancies have been dealt with and assured maintenance of high standards in future.

Allegations and findings:

On March 8, 2017 SEBI issued a Show Cause Notice (SCN) to the appellant alleging violation of AML/CFT policy under the Prevention of Money Laundering Act, 2002 ('PMLA' fort short) effected from July 1, 2005 as to why adjudication proceedings should not be initiated against

[20]Disclaimer: The summary of the instant orders is only representational in nature and does not hold any legal significance and cannot be relied upon or referred to as a precedence in any other case)

the appellant for violation of – (i) AML/CFT policy; (ii) Client Risk Categorization; and (iii) Suspicious Transaction Monitoring and Reporting. Following reply and opportunity of personal hearing etc. the impugned order was passed on July 31, 2017 whereby the appellant was found to have violated AML/CFT policy by delaying its proper implementation by a number of years and therefore imposed a penalty of ` 40 Lakh on the appellant. According to the impugned order, the appellant is alleged to have violated clause 11 of the Third Schedule of Regulation 20AA of the Securities and Exchange Board of India (Depositories and Participants) Regulations, 1996 ('DP Regulations' for short) for non-incorporation of the provisions of the (i) SEBI Master Circular no. CIR/ISD/3/2010 on AML/CFT dated December 31, 2010, (ii) Circular no. CIR/MIRSD/2/2013 issuing Guidelines on Identification of Beneficial Ownership dated January 24, 2013 and (iii) Circular no. CIR/MIRSD/1/2014 dated March 12, 2014, modifying the AML Circular.

The table given at pages 4 to 6 of the impugned order lists six violations committed by the appellant in terms of delay in implementation of the required policies and practices under anti-money laundering policy. Such delays ranged from 2 to 4 years. However, it was not disputed that though delayed, the appellant was in compliance with all the ingredients of the anti-money laundering policy as required under the extant SEBI Circulars.

Arguments:

The basic contention of the appellant was that the policy framed was more like procedural in nature to be incorporated in the internal policies of the appellant which had been done. As such, there had been no violation per se. However, without pressing this argument further, Counsel for the appellant submitted that the amount of penalty of Rs.40 Lakh imposed was too high given that the violations were only in the nature of procedural delays and did not adversely affect the investors in any manner. Further, in a few other similar matters the penalty imposed by SEBI was either Nil (in the matter of IFCI Financial Services Limited) or Rs.1.50 Lakh (in the matter of Triveni Management Consultancy Services Limited). However, in the case of the appellant despite proper implementation of the necessary directions of SEBI penalty of Rs. 40 Lakh had been imposed which was highly disproportionate for the alleged violations.

The respondent contended that the AML policy was to be implemented with full force given that they were emanating from international obligations and provided for under the Indian laws. Therefore, delay of several years for implementing each of the six noted violations cannot go unpunished.

Conclusion

Given the fact that, though belatedly, the appellant had implemented all the required policies and procedures on AML/CFT policy as stipulated under the various circulars of SEBI and by the penalty precedent set by SEBI itself, the Securities Appellate Tribunal was of the view that the penalty of Rs.40 Lakh imposed on the appellant was excessive. The Securities Appellate Tribunal, therefore, reduced the amount of penalty imposed on the appellant to Rs. 6 Lakh.

8.7 FIU-IND vs Paytm Payments Bank Limited

Paytm Payments Bank Ltd by virtue of operating as a payments bank, is a 'reporting entity' for the purposes of Section 2(l)(wa) and is registered as such with FIU-IND. A show-cause notice (SCN) numbered 9-55/2020/Compl/FIU-IND dated 14.02.2022, was issued to PayTM Payments Bank Ltd. (RE).

Issues for consideration

The inception of the current proceedings stems from the identification by law enforcement agencies of extensive illegal activity conducted by multiple businesses under the syndicate of individuals connected to a foreign state. The matter first came to light with the lodging of First Information Reports (FIRs) by the Cyber Crime Station of Hyderabad under relevant sections of the Indian Penal Code and the Telangana State Gambling Act in relation to the activities of certain business entities. The FIRs state that these entities and their network of businesses engaged in a number of illegal acts, such as organizing and assisting online gambling, and that the money obtained from these illegal operations that were proceeds of such criminal activities were routed and channeled through bank accounts maintained by the same entities with the Bank.

As part of its mandate to ensure effective implementation of Chapter IV of the PMLA, FIU- IND regularly examines the compliance levels of 'reporting entities' in the wake of any criminal conduct or fraud being reported to it or otherwise coming to light. In the course of such investigation, and as reported in the public domain, certain entities were found to have cheated lakhs of Indians through the offering of fraudulent services including prohibited gambling activities, dating services, and streaming. The proceeds of these fraudulent activities were subsequently remitted abroad. It came to light that several of the involved entities had made use of payment intermediaries to implement their fraudulent designs within the country.

Allegations and findings

The matter, and the responses of the Bank, were examined in detail by FIU-IND and it appears to be the case that the Bank has failed to discharge its obligations under Chapter IV of the PMLA. The Bank conveyed its response and after examining the material on record and the submissions made, the bank has been found to breach/violated the following relevant obligations:

Payout-related charges:

a) In respect of the failure of the Bank to put in place an internal mechanism to detect and report suspicious transactions in the manner prescribed under the PMLA and PML Rules including with reference to its Payout service and accounts of the entities in question. In violation of Section 12(1) of PMLA read with Rules 3(1)(0) and 7(3).
b) In respect of the failure of the bank to exercise ongoing due diligence with respect to its Payout service and accounts of entities in question relating to the same service in violation of Section 12(1) of PMLA read with Rule 9(12);
c) In respect of failure of the Bank to satisfy the requirements with respect to reliance on third-party KYC by relying on a non-compliant / unregulated entity in violation of Section 12 of PMLA read with Rule 9(2)(c) and Rule 9(2)(f).

Beneficiary account related charges:

a) In respect of failure to file suspicious transaction reports, in respect of 34 beneficiary accounts, in the manner, and within timelines, prescribed under the PMLA and PML Rules in violation of Section 12(1) of PMLA read with Rules 3(0) and Rule 8 of the PML Rules.
b) In respect of the failure of the bank to exercise ongoing due diligence with reference to the accounts of 34 beneficiaries which received proceeds from the Payout accounts of and entities in question in violation of Section 12(1) of PMLA read with Rule 9(12), PML Rules.

Order

After considering the written and oral submissions of the Bank, Director, FIU-IND, based on the material available on record, found that the charges against Paytm Payments Bank Ltd were substantiated. Consequently, the Director FIU-IND vide order dated 15 March, 2024 in exercise of his powers under Section 13 PMLA, imposed a total fine of Rs. Rs. 5,49,00,000 (Rupees Five Crore Forty-Nine Lakh Only) on the Bank with reference to the above violations committed by the Bank.

8.8 FIU-IND vs Virtual Digital Asset Service Provider Bybit Fintech Limited (Bybit)

Allegations and findings

The Financial Intelligence Unit-India (FIU-IND) in furtherance of the powers conferred upon the Director FIU-IND under Section 13(2)(d) of the Prevention of Money Laundering Act, 2002 (as amended) ("PMLA") has imposed a monetary penalty of Total ₹9,27,00,000 (Nine crore twenty-seven lakh rupees) on Bybit Fintech Limited (Bybit) a Virtual Digital Asset Service Provider (VDA SP) with reference to the violations of its obligations under the PMLA read with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Rules") issued thereunder and applicable guidelines and advisories issued by the Director FIU-IND.

As a Virtual Digital Asset Service Provider (VDA SP), Bybit Fintech Limited (Bybit) is classified as a 'reporting entity' under Section 2(1) (wa) of the Prevention of Money Laundering Act (PMLA). Bybit kept expanding its services in the Indian market without securing mandatory registration with the FIU-IND. The persistent and continuous non-compliance caused FIU-IND to block their websites to stop operations under the Information Technology Act, 2000 through the Ministry of Electronics and Communication Technology (MEITY).

It is noteworthy that FIU-IND had previously issued comprehensive Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Guidelines for Reporting Entities offering Services related to Virtual Digital Assets on March 10, 2023. Furthermore, a detailed circular regarding the registration of Virtual Digital Asset Service Providers as reporting entities was issued on October 17, 2023.

Findings and Order

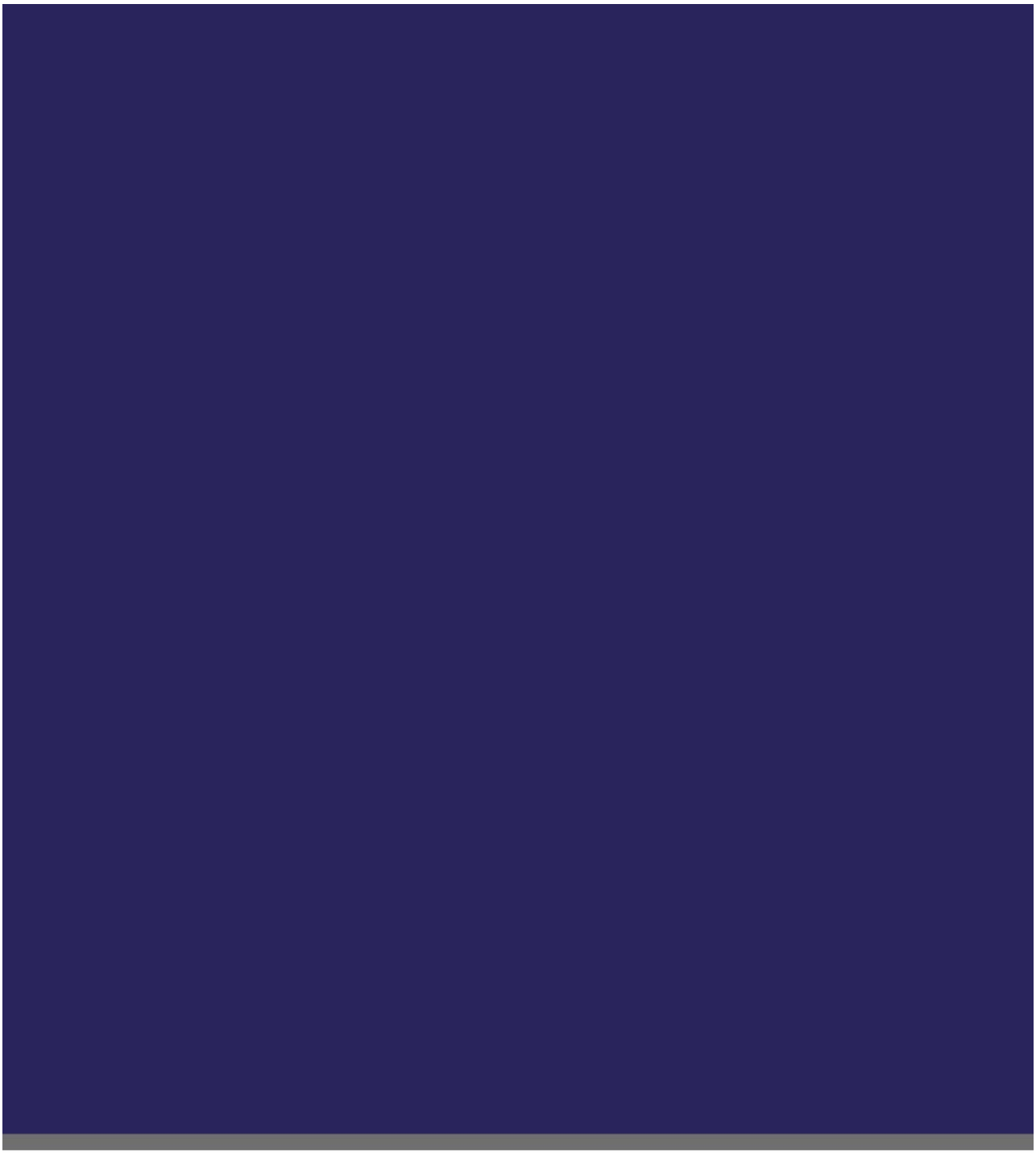
After conducting a thorough examination of both written and oral submissions from Bybit, Shri Vivek Aggarwal, the Director of FIU-IND, found Bybit liable of the charges for various violations. In an order dated January 31st, 2025, and exercising authority under Section 13 of the PMLA, it was unequivocally established that Bybit was in violation of Section 12(1) of the PMLA read with Rule 2(1)(h), Rule 7(2), Rule 8(2) Rule 8 (4), Rule 3(1)(D) and Rule 7(3) of PMLR, 2005. Consequently, a total penalty of Rs. 9,27,00,000 was imposed on Bybit.

Sample Questions

1. Which of the following activities should NOT to be done by a reporting entity?
   a) Raise an alert
   b) Investigate an alert
   c) Ignore an alert
   d) File a STR

2. As per Regulatory requirement, all intermediaries should:
   a) Have an Anti Money Laundering Policy
   b) Apply customer due diligence on risk sensitive basis
   c) Appoint a Principal Officer
   d) All of the above

3. Which of the following statements about the actions of an intermediary is TRUE?
   a) Should not classify clients into High, Medium and Low risk
   b) Should close STRs without giving appropriate reasons
   c) Have a system to identify clients as a potential PEP (Politically Exposed Person)
   d) Monitor transactions without considering AML & CFT provisions.



NATIONAL INSTITUTE OF SECURITIES MARKETS

NISM Registered Office
5th floor, NCL Cooperative Society,
Plot No. C-6, E-Block, Bandra Kurla Complex,
Bandra East, Mumbai, 400051
Tel: +91-22-41738811

NISM Campus
Plot No. IS 1 & 2, Patalganga Industrial Area,
Mohopada, District Raigad,
Maharashtra–410222
Tel: +91-2192-668300

NISM Bhavan
Plot No. 82, Sector–17,
Vashi, Navi Mumbai, Maharashtra–400703
Tel: +91-22-66735100/5101
Fax: 022-66735110

www.nism.ac.in