Developing an AML-Compliant Risk Assessment Framework for SEBI Registered Intermediaries

In a world where financial systems are increasingly interconnected, the scourge of money laundering poses a significant threat to global economies. According to an IMF study, the magnitude of money laundered worldwide is estimated to range from 2% to 5% of the global GDP, potentially equating to a staggering $2 trillion. To put this into perspective, at its highest estimate of 5%, money laundering represents the fifth-largest economy globally, surpassing the GDP of India. Even at the lower estimate of 3%, it would still rank as the tenth-largest economy, eclipsing the combined GDP of the bottom 150 nations.

CS Shaily Gupta, ACS

Practising Company Secretary, Chartered Accountant
Founder of SHAILY & CO.,
Navi Mumbai
shaily.co@outlook.com

INTRODUCTION

In a world where financial systems are increasingly interconnected, the scourge of money laundering poses a significant threat to global economies. According to an IMF study, the magnitude of money laundered worldwide is estimated to range from 2% to 5% of the global GDP, potentially equating to a staggering $2 trillion. To put this into perspective, at its highest estimate of 5%, money laundering represents the fifth-largest economy globally, surpassing the GDP of India. Even at the lower estimate of 3%, it would still rank as the tenth-largest economy, eclipsing the combined GDP of the bottom 150 nations.

To combat this pervasive issue effectively, it is crucial to comprehend the concepts of money laundering, reporting entities including registered intermediaries in the financial ecosystem.

MONEY LAUNDERING

The term "money laundering" originates from the concept of cleansing illicit funds, much like one might launder dirty clothing to make them appear clean and untainted. However, the history of this term bears a fascinating connection to the notorious American mafia figure, Al Capone. Capone, a key figure in organized crime during the Prohibition era, ingeniously established laundry businesses across the United States. These laundromats operated as cash businesses, allowing him to convert illicit earnings into legitimate income. Thus, the term "money laundering" was coined.

According to the Prevention of Money Laundering Act (PMLA) 2002, "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."

Here, '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."

Money laundering typically involves three distinct stages:

1. **Placement:** The initial phase involves the physical disposal or placement of the proceeds of crime into the financial system or retail economy. Common typologies or methods in this stage include structuring cash deposits, loan repayments, cash smuggling, gambling, high-value item purchases (e.g., foreign exchange, gold, diamonds), commingling laundered cash with legitimate businesses (e.g., restaurants, entertainment), and down payments for real estate acquisitions.

2. **Layering:** The objective of this stage is to obscure the source of funds by executing a series of financial transactions that create layers of complexity, thus concealing the audit trail and providing anonymity. Electronic funds transfers have made this stage considerably easier. Common methodologies at this stage encompass account transfers within and across institutions, wire transfers to foreign jurisdictions, the use of shell companies, conversion of cash into monetary instruments, and investments in stocks and real estate.

3. **Integration:** The final stage involves integrating ill-gotten funds with legitimate assets, thereby giving them the appearance of legitimacy and incorporating them into the net worth. Activities at this stage often appear as routine business and personal transactions. Common methodologies include the purchase of investment and luxury assets (e.g., property, artwork, jewellery, high-end automobiles), investments in legitimate businesses, and capital market activities.

REPORTING ENTITIES

To combat money laundering effectively, the PMLA imposes obligations on specific reporting entities, which include:

- Banking companies,
- Financial institutions,
- Intermediaries of the securities market,
- Persons engaged in designated business or professions.

These entities are required to verify the identity of clients, furnish information, and maintain records.

As defined in Section 2(n) of the PMLA, an "intermediary" includes various entities registered under the Securities and Exchange Board of India Act, 1992 (Additionally, it encompasses entities recognized or registered under the Forward Contracts (Regulation) Act, 1952, intermediaries registered by the Pension Fund Regulatory and Development Authority, and recognized stock exchanges under the Securities Contracts (Regulation) Act, 1956.

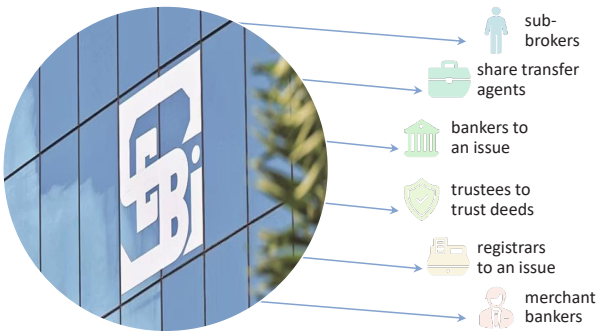

Figure 1- Intermediaries registered under the Securities and Exchange Board of India Act, 1992; Author's Presentation

The role of registered intermediaries in the securities market is crucial but also susceptible to money laundering risks. Various factors contribute to this vulnerability. The factors are enlisted in the Figure 2 below. It is essential for reporting entities, especially registered intermediaries, to be vigilant and proactive in mitigating these risks to maintain the integrity of the financial system.

Figure 2- Susceptibility of securities markets to money laundering risks; Author's presentation

NEED FOR RISK BASED CLIENT DUE DILIGENCE

The Securities Board of India underscores the importance of adopting a risk-based approach in its guidelines. These guidelines mandate registered intermediaries to conduct a thorough risk assessment. The aim is to identify and implement effective measures to counter money laundering and terrorist financing risks. This process involves evaluating various factors, including client profiles, the countries or regions involved, transaction characteristics, and payment methods used.

- Documentation- Moreover, this risk assessment should take into account all relevant risk factors before determining the overall risk level and the most suitable mitigation strategies. It's essential to document this assessment, regularly update it, and make it accessible to competent authorities and self-regulating bodies as needed. The requirement for proper documentation underscores the significance of this exercise in the financial sector.
- Defining risk thresholds- The risk-based approach in managing AML/CFT (Anti-Money Laundering/ Counter Financing of Terrorism) categorizes clients as either higher or lower risk based on specific circumstances. Risk- assessments by registered intermediaries should carefully consider relevant risk factors when determining the overall risk level and the most suitable mitigation approaches.
- Risk attuned due-diligence- For clients falling into higher risk categories, enhanced due diligence measures should be adopted. Conversely, lower risk categories may warrant a simplified client due diligence process. A risk-based approach offers a pragmatic way to accomplish more with fewer

constraints, whether due to budget limitations or the availability of qualified personnel and technology resources.

CATEGORIES OF POTENTIAL RISKS FOR REGISTERED INTERMEDIARIES

1. **Distribution/Channel Risks:** These risks involve doing business with entities suspected of criminal activities, located in risky countries, serving risky customers, having a history of not following the rules, appearing negatively in the media, lacking proper anti-money laundering (AML) training, or having weak controls. Dealing with such entities can expose businesses to money laundering and terrorism financing risks.
2. **Country/Geographic Risks:** These risks arise from dealing with jurisdictions that provide funding for terrorism, host designated terrorist organizations, exhibit high levels of organized crime and corruption, are subject to sanctions or embargoes, or have weak governance, law enforcement, and regulatory regimes. Operating in or with entities from such regions increases the likelihood of AML and terrorism financing risks.
3. **Product/Service/Transaction Risks:** These risks involve products, services, or transactions that offer anonymity, have extensive geographical reach, possess unusual complexity or structure, lack an obvious economic purpose, allow unrestricted value transfer (especially to high-risk areas), employ new technologies or payment methods, are prone to fraud and market abuse, involve the purchase of securities using physical cash, resemble bank-like products, include unrelated third parties, receive funding from high-risk jurisdictions, or deal with penny and illiquid stocks. Such elements can introduce vulnerabilities and potential AML risks.
4. **Customer/Investor Risks:** These risks stem from clients who have been sanctioned for AML/FT non-compliance, are considered Politically Exposed Persons (PEPs)[1] or have close associates with political prominence, derive income or wealth from high-risk jurisdictions, reside in high-risk areas, act on behalf of third parties with non-transparent motives, evade or provide misleading information, are linked to adverse media coverage, generate a high number of Suspicious Transaction Reports (STRs), maintain complex and rapidly changing legal structures, have exposure to sanctions, or possess non-transparent ownership structures. Dealing with such clients can elevate AML and terrorism financing risks.

DESIGNING A COMPLIANCE FRAMEWORK

In managing Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) risks, developing internal policies and procedures backed by a robust compliance framework is essential. This includes:

> As defined in Section 2(n) of the PMLA, an "intermediary" includes various entities registered under the Securities and Exchange Board of India Act, 1992 (Additionally, it encompasses entities recognized or registered under the Forward Contracts (Regulation) Act, 1952, intermediaries registered by the Pension Fund Regulatory and Development Authority, and recognized stock exchanges under the Securities Contracts (Regulation) Act, 1956.

- **Understanding the Rules:** Identifying and interpreting relevant AML and CFT rules and regulations to ensure a clear understanding of compliance requirements.
- **Using Technology:** Investing in advanced technology solutions to enhance compliance capabilities.
- **Rule Adherence:** Strictly following the regulations applicable to the entity's operations.
- **Measures and Procedures:** Developing measures and procedures to prevent money laundering and terrorist financing.
- **Customized Policies:** Tailoring policies to consider the specific nature of the business, client profiles, and organizational structure.
- **Senior Management Involvement:** Ensuring full commitment from senior management in establishing appropriate policies and procedures.
- **Regular Review:** Continuously reviewing policies and procedures with the assistance of an independent party.
- **Client Acceptance Policies:** Implementing policies for client acceptance and due diligence, including proper identification requirements.
- **Effective Communication:** Clearly communicating compliance policies to all levels of management and relevant staff.
- **Statutory and Regulatory Compliance:** Ensuring strict compliance with relevant statutory and regulatory requirements.
- **Internal Oversight:** The internal audit or compliance functions play a crucial role in ensuring ongoing compliance.
- **Board Approval:** These policies and procedures require approval from the Board, highlighting their importance.

1. *In financial regulation, a politically exposed person is one who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence they may hold.*

ENSURING ONGOING AML TRAINING FOR EMPLOYEES

Regular staff training is vital for ensuring everyone understands and follows Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and Know Your Customer (KYC) requirements. These training programs should cover topics like money laundering and terrorist financing techniques, global standards, and updates in these fields. To keep track of employee training, organizations should maintain records that show when and how training was provided, who attended, and how often. Different training methods, like certified courses, in-house sessions, online modules, and awareness sessions, can be used. Keys areas to be included in the training are explained in Figure 3 below. Lastly, any changes in AML/CFT laws or company policies related to these matters must be communicated to the relevant employees promptly.

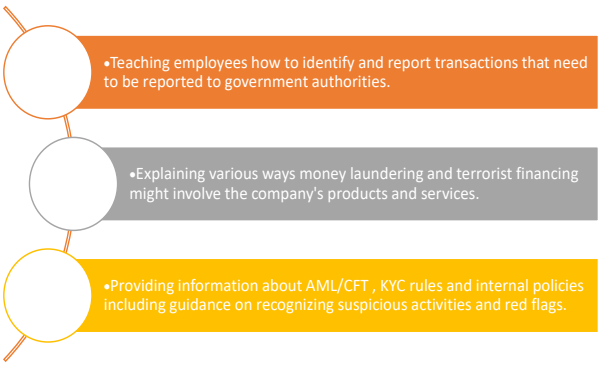

Figure 3; Key areas to include in AML and KYC training; Author's Presentation

ESTABLISHING AN INDEPENDENT AUDIT FUNCTION

An independent AML audit is like a check-up for a company's Anti-Money Laundering (AML) plan. It's not about money, but about making sure the company has a proper AML program and is actually following it. During an AML audit, the following things are usually examined:

- Reviewing the company's AML compliance program document.
- Testing if the AML Policy and Procedures are being put into action.
- Checking how well the Customer Identification Procedure (CIP) is working.
- Examining transactions to see if there are any issues.
- Investigating whether the company is following OFAC (Office of Foreign Assets Control) regulations.
- Looking at reports related to financial crimes, like Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs).
- Evaluating the effectiveness of AML training.
- Checking the automated monitoring methods and management information systems.
- Reviewing previous audit reports to see if recommended changes were made effectively.

WHO CAN CONDUCT THE AML AUDIT

An AML audit can be done by company employees who are not involved in areas where money laundering concerns might happen or by an external, independent third party. This means that the audit cannot be done by the company's AML compliance officer or their team. Smaller businesses often choose independent third parties because they may lack the expertise or resources to do it internally.

CONCLUSION

In the world of professionals like Company Secretaries (CS), a realm of immense opportunity beckons. CS experts play a pivotal role in shaping internal policies, constructing resilient compliance frameworks, conducting vital independent audits, and imparting essential training. By pioneering streamlined mechanisms for reporting suspicious transactions and harnessing the power of technology, we have the potential to revolutionize how we combat financial crime.

These efforts not only fortify our financial institutions but also empower authorities like the FIU-IND (Financial Intelligence Unit of India)[2] to carry out their vital functions with greater efficiency. Our dedication to understanding and implementing AML provisions is not just theoretical; it translates into tangible results. It can significantly reduce economic losses and protect the well-being of our nation's economy.

So, as CS professionals, let's recognize the real impact we can create. Let's seize this opportunity to drive positive change, to safeguard the financial integrity of our nation, and to ensure a brighter future for all. The path ahead is tangible, and our actions today resonate for generations to come.

REFERENCES:

i. unodc.org.

ii. taxmann.com

iii. fiuindia.gov.in

[2] *Financial Intelligence Unit – India is an organisation under the Department of Revenue, Government of India which collects financial intelligence about offences under the Prevention of Money Laundering Act, 2002.*