BANKING INSTITUTIONS AND ANTI-MONEY LAUNDERING COMPLIANCE IN INDIA: A CRITICAL ANALYSIS OF THE LEGAL AND INSTITUTIONAL FRAMEWORK

Vidhika Roy Parihar, BA. LL.B., The Law School, University of Jammu

ABSTRACT

Money laundering has become one of the major threats to the integrity, transparency, and stability of modern financial systems. Presently financial transactions grow more digital and interconnected across borders, banking institutions play a key role in stopping the movement and legitimization of illegal funds. In India, the anti-money laundering (AML) framework mainly follows the Prevention of Money Laundering Act, 2002 (PMLA). This framework is backed by the institutions such as the Reserve Bank of India (RBI), the Financial Intelligence Unit–India (FIU-IND), and various enforcement bodies. Banks serve as the first line of defense against money laundering. They do this by enforcing customer due diligence, following Know Your Customer (KYC) rules, monitoring transactions, reporting suspicious activities, and keeping records.

This paper examines the role of banks within India's AML framework and assesses the effectiveness of the legal and institutional measures aimed at fighting money laundering. The study looks at the laws governing AML compliance, including key parts of the PMLA, the Banking Regulation Act of 1949, and the Reserve Bank of India Act of 1934. It also reviews the institutional framework, which includes the RBI, FIU-IND, Enforcement Directorate, adjudicatory bodies, and financial institutions. Special focus is given to the operational tasks required by banks and how they help detect, prevent, and report suspicious financial activities. It evaluates the important court rulings on the relationship between banks and enforcement agencies in money laundering investigations. It also highlights major challenges to AML enforcement, such as low conviction rates, technological limitations, informal financial networks, poor coordination among agencies, and the growing complexities from digital assets and cross-border transactions. Based on these findings, the study suggests several reforms, including updating technology, improving coordination among institutions, creating specialized adjudicatory bodies, and enhancing international cooperation which is elemental for safeguarding the integrity of India's financial system.

1.Introduction

The financial stability and integrity of the banking system of the country are the prerequisites for sustainable economic growth and development. Banking institutions are the backbone of contemporary economic activities. The financial health of a country is most important for its growth and development. These institutions carry a heavy workload in running a nation, not only regulating the wealth of the nation but also securing the nationals. The growth of modern banking systems and rapid technological advancements have significantly transformed the way financial transactions are conducted across the world. However, alongside these developments, banking systems have also become increasingly susceptible to exploitation by individuals and organisations seeking to conceal illegally obtained wealth through legitimate banking channels.

Money laundering is one such misuse of the banking institution. It is the illegal process of taking hefty sums of money gathered by criminal activity and making it appear as though it came from a legitimate source. The offence of money laundering not only allows organised crime, drug trafficking, tax evasion, terror financing, and financial fraud but also hampers the nation's financial soundness and market stability. The banking systems of a country become primary channels for such activities through which illicit funds are introduced, layered, and then ultimately integrated into a whitewashed version. This offence is primarily dealt by the Indian legislation named The Prevention of Money Laundering Act, 2002. This enactment was introduced to combat and prevent money laundering. The approach of the act is simple; it prevents, provides deterrence, and enforces compliance.[1]

The increasing menace of money laundering in India led to the development of an extensive anti-money laundering framework. It includes certain legislative, regulatory and institutional mechanisms, specifically the enactment of The Prevention of Money Laundering Act, 2002; The Banking Regulation Act, 1949[2]; The Reserve Bank of India Act, 1934[3], along with certain other regulations and monitoring systems. This exhibits the efforts of the state to fortify financial security and reduce gaps within the banking sector.

[1]The Prevention of Money Laundering Act, No. 15 Of 2003, India Code (2003).
[2] The Banking Regulation Act, No. 10 of 1949, India Code (1949).
[3]The Reserve Bank of India Act, No. 2 of 1934, India Code (1934).

With the evolution of technology and enhanced globalisation, the banking sector introduced major reforms and anti-money laundering setups, which include customer identification and KYC (know your customer), transaction monitoring, and suspicious transaction reporting, etc. Despite these legal and regulatory mechanisms, repeated banking frauds, compliance failures, cross-border financial crimes, financial scandals, and emerging technological challenges continue to lay bare the weaknesses within the existing anti-money laundering framework. The rise of digital banking, online transactions, shell companies, and virtual assets has further complicated regulatory enforcement and increased the intricacy of financial investigations.

This study critically examines the role played by banking institutions in preventing money laundering within India's anti-money laundering framework. The study analyses legal obligations imposed upon banks, evaluates the effectiveness of existing compliance mechanisms, investigates practical challenges affecting the implementation of anti-money laundering laws within the Indian banking system and identifies actionable reforms to strengthen the AML framework.

2. Concept and process of money laundering

2.1 meaning and concept of money laundering.

Money laundering poses a huge peril to the financial organisation of a nation, as it allows the illegitimate capital to enter a legitimate economy and creating market disability. It refers to the process through which proceeds generated from unlawful activities are disguised, transferred, transformed, or integrated into legitimate financial systems to mask their illicit origin. The core ideology behind money laundering is not merely the concealment of illegally obtained wealth but the creating a façade of legitimacy that enables criminals to utilize such proceeds without drawing regulatory or law enforcement attention.

Section 3 Of The Prevention of Money Laundering Act, 2002, provides for 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 and projecting it as untainted property shall be guilty of offence of money laundering." This offence of money laundering has evolved into a global financial crime affecting both developed and developing economies and the increasing globalization of financial markets, expanding web of digital transactions, and growth of sophisticated banking systems have significantly amplified opportunities for criminals to transfer illegal funds through formal financial institutions.

Mounting rates of financial frauds, crimes associated and technological advancements, looking into anti money laundering framework is prioritized by the government, financial institutions and regulatory bodies. The banking sector plays a pivotal role in enforcing AML measures, acting as the first line of defence against such illegal transactions. But the challenges of regulations, compliance burdens and the dynamic nature of financial crimes necessitate continuous reforms in the implementation of PMLA provisions. The enactment empowers enforcement agencies, strengthens regulatory mechanisms, and imposes stringent compliance obligations on financial institutions, particularly banks which are key players in preventing illicit financial flows. The banking sector plays a critical role in the enforcement of AML (anti-money laundering) framework as banks are the primary conduits through which money laundering occurs. Criminals exploit banking systems for illegal financial activities, such as layering illicit funds, disguising the origin of proceeds from crimes such as drug trafficking, fraud, and tax evasion. To ease these risks, banks are required to implement robust AML policies, conduct know your customer(KYC) procedures, monitor transactions, report suspicious activities, and join forces with regulatory bodies such as the Reserve Bank of India (RBI), the Financial Intelligence Unit – India (FIU-IND), and the Enforcement Directorate (ED). To act in accordance with The Prevention of Money Laundering Act (PMLA), 2002, financial institutions especially the banking sector must take a highly tactical standpoint. This requires them to elevate operational transparency, fortify their inner compliance frameworks, and actively block criminals from exploiting their banking networks for illegal asset transfers. Then again, integrating these legal mandates into daily banking operations presents severe snags. Financial firms frequently struggle with heavy compliance overheads, conflicting regulatory frameworks, evolving digital vulnerabilities, and the intricate nature of international fund tracking all of which severely complicate modern anti-money laundering initiatives[4].

2.2 Process of money laundering[5]

Placement

[4] Aryan Sisodia, *The Prevention of Money Laundering Act (PMLA) and Its Role in Banking*, 7 Indian J.L. & Legal Res. 2854 (2026).

[5] Urveshi, *Money Laundering in India: Concept, Legal Provision and Effect* 1–17 (Galgotias Univ. Sch. of Law, Working Paper, 2021).

Placement is the physical entry point into the financial system of bulk, illicit cash. More often than not, illegal capitals are placed in a manner that avoids detection by banks and law enforcement agencies, typically as deposits into commercial bank accounts through structured deposits, nominee names, or front companies**.**

Layering

Layering involves separating criminal proceeds from their illicit source through complex, multi-tiered financial transactions premeditated to mask the audit trail and provide anonymity. With commercial banks, funds are moved with high speed. Funds are speedily transferred between bank accounts, altered into different foreign currencies, or wired across international borders to unknown offshore jurisdictions.

Integration

Integration is where the white-washed funds are reintroduced to the mainstream economy as legitimate funds. The capital re-enters the financial system disguised as lawful business revenue or investment capital. Instances of legal veils for integration include real estate purchases, capital market investments, e-commerce sales, and cash-intensive industries such as the hospitality or luxury retail industry.

2.3 Methods[6]

Smurfing

Smurfing also known as structuring, is a money laundering technique in which unlawful outflows are split up into smaller sums and transferred into various financial organizations or bank accounts. This is done to get around financial restrictions that mandate banks to record weighty transactions, usually those that surpass a predetermined level. Smurfs, or people operating on their behalf, are used by criminals to make several minor payments or purchases, frequently utilizing more than a few accounts or institutions. They avoid drawing the attention of authorities by keeping transactions below the reporting threshold.

[6]LexisNexis, *Examples of Money Laundering Techniques*, Compliance & Risk Due Diligence Blog (May 4, 2023), https://www.lexisnexis.com/blogs/gb/b/compliance-risk-due-diligence/posts/examples-money-laundering.

After the money has been fittingly deposited, it is often moved to different accounts or mixed up with other money, which further skins where it came from.

Smurfing can be a successful money laundering method despite its seemingly forthright nature, especially when numerous Smurfs are involved. However, financial institutions and law enforcement organizations have created means and instruments to identify and halt smurfing, including tracking transaction trends and using sophisticated algorithms to spot dubious activities.

Smuggling cash in bulk

An infamous instance of money laundering is bulk cash smuggling, which is the actual movement of considerable amounts of illegal money across global peripheries. Criminals use this technique to get around anti-money laundering (AML) regulations by avoiding the inspection by the regulatory bodies and financial institutions.

Trade-based laundering

Trade-based laundering (TBL) is a method of money laundering whereby criminals transport money across borders under the semblance of legitimate business transactions by manipulating the value, volume, or type of commodities being exchanged. This approach may entail overcharging or undercharging, manipulating documentation like invoices and customs declarations, or misrepresenting the type or quality of products.

Authorities find it puzzling to identify and stop this type of money laundering due to the complexity of (TBL) and the volume of international trade. Shell companies, intermediaries, and offshore financial centres are frequently used by criminals to disassociate themselves from their illegal activities and add layers of complexity.

Real estate laundering

Real estate laundering is a common example of money laundering where criminals invest illegal assets into the property market, cloaking the true origin of their wealth. In this method, illegitimate gains are channelled into buying, selling, or renting real estate properties to create the frontage of legitimate financial transactions.

Shell companies and trusts

Shell companies and trusts are convenient tools in money laundering schemes because they provide a complex cover-up to conceal illicit funds. By setting up these entities, frequently in offshore jurisdictions, criminals can skilfully screen the true source of their wealth. Both shell companies and trusts take advantage of holes in the financial system and international regulations to continue money laundering activities. Shell companies, which are usually devoid of legitimate business operations, act as a red herring for the trail of money by enabling the transfer of funds between accounts, giving the appearance of legitimate transactions. The complexity of the financial web becomes more difficult for authorities to track down the money.

Cyber laundering

Cyber laundering is a strong-growing process of money laundering, using the digital world to hide the source of dirty money. With the rapid development of technology, criminals can Develop new ways of concealment, making the work of traditional detection methods more difficult.

Cyber laundering makes all-embracing use of digital currencies and cryptocurrencies. Criminals use blending services to mix their illicit money with legitimate money. This complicates the ability of law enforcement to track the original funds back to their source. Online gaming platforms have also become popular dais for cyber laundering. Virtual assets, in-game currencies and items are often transferred across countries creating a labyrinth of transactions that is difficult for investigators to comprehend.

3. Legislative foundations: the statutory mandates on banking institutions

Money laundering is a widespread problem in today's context. To tackle the issue in hand the Indian legislature came up with certain enactments, mechanisms and regulations. The major acts include The Prevention of Money Laundering Act, 2002; The RBI Act, 1934 and The Banking Regulation Act, 1947, other than these certain regulations and guidelines also exist as India's anti money laundering framework.

The Prevention of Money Laundering Act 2002[7]

It is the core legislation dealing with the offence of money laundering. It predominantly focuses on the deterrence and preventive measures to combat the offence. The act is arranged into ten chapters and seventy-five sections. It deals with proceeds of crimes, attachment, adjudication, and confiscation thereof, obligations of banking institutions and various authorities.

Section 3 – offence of money laundering.

This section highlights the definition of the offence of money laundering and what essentially constitutes this offence. It says "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 1 [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."

The provision criminalizes activities like concealment, possession, acquisition, use, projection claiming proceeds of crime as property. This has resulted in removing the vagueness of the offence and enhanced the enforcement powers. The provision has created a vast legal net expanding the scope of involvement.

Section 4. Punishment for money laundering.

This section is based upon the deterrence philosophy. It highlights the seriousness of the offence and the regulation of the offence within the Indian society. It removes the court's discretion and sets up a statutory ceiling of punishment. The term for the punishment must be at least three years and extendable up to seven years, also liable for a fine. Capping a fine at 500,000 inr was highly ineffective when dealing with multi-crore systemic swindles or transnational drug syndicates. By deleting this phrase, the legislature gave the judiciary the authority to impose **uncapped, unlimited financial penalties**. The fine can now scale proportionally to the actual volume of the "proceeds of crime" unearthed. The maximum jail sentence from 7 to 10 years for drug-related laundering, the law explicitly recognizes the nexus between narcotics trafficking, organized syndicate operations, and the threat of narco-terrorism

[7] The Prevention of Money Laundering Act, No. 15 Of 2003, India Code (2003).

to national security.

Section 5 attachment of property involved in money laundering.

This section allows the enforcement directorate to temporarily seize the assets suspected of "proceeds of crime" for up to 180 days before a person is convicted. It is a weapon in hands of the enforcement agencies to intervene in the banking lifecycle by freezing the capital. The money launderers do not usually keep their proceeds in cash instead they integrate it into commercial banking infrastructure under this section ED issues an attachment order which a bank is legally mandated to oblige to. When the ED provisionally freezes a corporate account under section 5, it triggers immediate operational paralyses such as payroll failures and credit defaults, the burden of proof is reversed under section 24 of the PMLA, banks are legally blocked from releasing these funds, forcing the account holder to navigate long, complex administrative litigation just to prove their legitimate income pipelines.

Section 12 reporting entities and record keeping.

The section 12 of the act establishes a statutory obligation upon the reporting entities which includes transaction records, mandatory reporting of such records to the director, client identity maintenance, and statutory retention periods.

These reporting entities includes banking companies, financial institutions, intermediaries, and certain designated professionals. It is one of the important provisions amongst the anti-money laundering framework since they are meant to maintain a comprehensive record of all transactions, furnish information regarding all transactions whether successful or merely attempted to the director of the financial intelligence unit (FIU). This provision forces the required institutions to play an initiative-taking role and spot any sceptical activities before they occur.

The section also gives power to the director to access information from such established reporting entities and grants an investigative power to gather intelligence. The entities are under statutory obligation to furnish all such information to the authority. This section of the act enhances the enforcement mechanism, while highly effective for data tracking and reporting of illicit dealings, it minimizes conventional consumer financial privacy by centralizing data access powers under the executive branch.

Section 13 powers of director to impose fine.

This section allows the director to hold the power to call for any systematic records or additional transaction files necessary to audit. It empowers the enforcement authority to initiate inquiry which aims to verify whether a banking company, financial institutions or intermediaries failed to abide by with statutory obligation laid under chapter IV. If upon concluding the inquiry any deficiencies or a deliberate non-compliance by reporting entities is observed, the director may, by an order, impose a monetary penalty on such reporting entity or its designated director on the board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure. This provision establishes a system of surveillance over the banking institutions not only holding individual accountable but as also the institution. It surely creates element for responsibility within the institution to comply with the provision of the act and remain answerable to prescribed authority.

Section14 no civil or criminal proceedings against reporting entities, its directors, and employees in certain cases.

This section creates a statutory safe harbour that allows reporting entities to fulfil their financial intelligence reporting duties without threat of legal action. It creates a complete legal immunity for commercial banks, their directors and front-line compliance staff when they furnish the records, cash transaction reports (CTR) or suspicious transaction report (STR) to the director of the financial intelligence unit- India (FIU-IND). This provision somehow balances the strict regulatory compliance requirements over the banking institutions and paves way for protection of privacy of individuals and their financial data.

3.2 Supplementary Legislations

The Banking Regulation Act, 1947[8]

The PMLA, 2002, mandates for reporting entities, the actual execution, monitoring and administrative enforcement of these rules within commercial banking operations are carried by The Banking Regulation Act (bra), 1947. This enactment bridges the gap between operational requirements and institutional security controls by utilizing the powers of the Reserve Bank of

[8] The Banking Regulation Act, No. 10 of 1949, India Code (1949).

India (RBI) to enforce compliance.

Section 35A- power of the RBI to give directions.

This section empowers the RBI to issue binding directions to banking companies in public interest, to prevent the affairs of any banking company from being conducted in a manner detrimental to interest of the depositors or to secure the proper management of any banking company. For example, the master direction- know your customer (KYC) directions, 2016, these guidelines were issued to combat the offence of money laundering and improve customer identification and due diligence processes. The core ideology behind the section is protection of public and public money. The directions issued are duty-bound, therefore creating a regulatory framework and setting up RBI as sole trailblazer.

Section 47A- RBI to impose penalties.

To ascertain the compliance of the directions issued by the RBI, the act provides an enforcement mechanism under this section. The RBI can impose severe monetary penalties directly on the banking institutes for non-compliance ensuring that these banking institutions are administered and regulated accordingly.

The Reserve Bank of India Act, 1943[9]

This enactment is another important part of India's anti money laundering framework as it not only looks into the regulation of the banking institutions but also the alternative avenues like the non-banking sectors. Sections 45JA and 45L of the RBI act provide the legal framework to prevent shadow banking. Section 45JA confers power to the RBI to determine policy and give binding directions to NBFCS (non-banking financial companies) in the public interest or to protect depositors. Section 45L extends this scope and permits the central bank to regulate and direct any bank concerning its credit system and operations. These sections help the RBI anchor its master direction, know your customer (KYC) direction, 2016 directly onto the non-banking ecosystem. These again establishes RBI as guardian of the depositors and a regulatory body for the non-banking sectors.

[9]The Reserve Bank of India Act, No. 2 of 1934, India Code (1934).
[10]FATF, Anti-money laundering and counter-terrorist financing measures – India, 2023.

3.3 International Benchmarks: Aligning Indian Banking with FATF Recommendations.[10]

The financial action task force (FATF) is the leading global inter-governmental body that sets transnational standards to prevent money laundering, terrorist financing, and the spread of weapons of mass destruction. The '40 recommendations' are at the heart of the international regulatory framework of the FATF. These recommendations set the legislative and operational standards to implement by member states on their territory.

Commercial banking institutions are the primary entry point into the formal financial ecosystem, and the FATF framework places its most significant preventive compliance burdens on the banking sector. Recommendations 10 and 11: banks are required globally to perform rigorous customer due diligence (CDD), to maintain ongoing monitoring of high-risk relationships, especially those involving politically exposed persons (PEPs) and to retain detailed transaction records for a minimum of five years to provide a clear forensic paper trail for international law enforcement agencies.

For domestic banking institutions, FATF compliance is not a theoretical exercise but a hard operational necessity that unswervingly impacts international capital liquidity and credit standing. To ensure global compliance, the FATF performs a vigorous peer-review process called the mutual evaluation report (MER). If a country's banking regulatory system is systemically lacking in enforcement or not adequately capturing illicit cross-border flows, the FATF can put that jurisdiction on its high-risk compliance lists, known as the "grey list" or "blacklist" in common parlance. International correspondent banks do regularly sever financial ties, international wire transactions are heavily scrutinized, and the overall cost of cross-border compliance increases. This shows how much a country's macroeconomic health depends on the compliance discipline of its banks.

4. The Institutional Framework[11]

The effectiveness of any anti-money laundering (AML) framework depends on the existence of a strong institutional framework to prevent, detect, investigate, and prosecute money laundering activities. In India, the prevention of money laundering act, 2002 (PMLA) provides for a comprehensive institutional mechanism of regulatory authorities, enforcement agencies,

[11] Bijay Agarwal, *Decoding Money Laundering: A Comprehensive Analysis of India's Regulatory Framework*, 5 **Ind. J. Legal Rev.** 509, 509–18.

adjudicatory bodies, and financial institutions. Among these stakeholders, banking institutions play a pivotal role as the primary concierges of the financial system and the first line of defence against money laundering.

4.1 **Reserve Bank of India** (RBI)

A major player in India's AML framework is the reserve bank of India (RBI). The Reserve Bank of India (RBI) is the regulator of banks and financial institutions and lays down policies to ensure that the banking system is not misused for money laundering.

The reserve bank of India's (RBI) master directions on know your customer (KYC), customer due diligence (CDD) and anti-money laundering standards stipulate that banks should verify customer identities, identify the beneficial ownership, maintain transaction records, monitor suspicious activities, and implement risk-based compliance mechanisms.

The RBI also carries out inspections and compliance reviews to ensure AML obligations are being observed. In case of non-compliance, RBI may impose penalties and regulatory sanctions. Thus, the RBI is the main supervisory authority ensuring that the banking institutions have effective AML controls.

4.2 Financial Intelligence Unit- India (FIU-IND)

The financial intelligence unit – India (FIU-IND) was established in 2004 as the central national agency responsible for receiving, analysing, and disseminating financial intelligence relating to suspect transactions. FIU-IND is the vital link between reporting entities and enforcement agencies.

Under PMLA and other laws, banks are deemed as reporting entities and are required to submit suspicious transaction reports (STRs), cash transaction reports (CTRs) and other specified reports to FIU-IND. The unit scrutinizes these reports for patterns suggestive of money laundering and shares actionable intelligence with agencies like the Enforcement Directorate, Central Bureau of Investigation (CBI) and law enforcement agencies.

Banks, being the main source of financial transaction data, are critical to enable FIU-IND to detect suspicious financial activities and combat money laundering effectively.

4.3 Enforcement Directorate (ED)

The Enforcement Directorate is the principal agency to enforce the provisions of the PMLA, 2002. It falls under the department of revenue, ministry of finance. The directorate is authorised to investigate offences of money laundering, conduct search and seizures, provisionally attach properties derived from crime, arrest accused persons and initiate prosecution before special courts.

The role of the ED is closely associated with banking institutions. Banks routinely provide transaction records, account details, KYC details and suspicious transaction reports (STRs) that help the ED to trace the proceeds of crime. Such cooperation is of utmost importance for the investigations and for the prevention by banking institutions of the integration of illicit funds into the legitimate economy.

India's AML framework is run by the coordinated actions of the ED, the FIU-IND, the RBI, the adjudicating authority, the appellate tribunal and the special courts. Banking institutions lie at the centre of this framework, creating, monitoring and reporting the financial data needed to detect suspicious activities.

Anti-money laundering scheme is effective only when banks know their customer, carry out customer due diligence, maintain records of transaction, monitor unusual transaction and promptly report suspicious transaction to regulatory authorities. The investigation and prosecution of money laundering is, evidently, the responsibility of the enforcement agencies and the courts. But it is the banks which provide the first and most critical institutional line of defence against money laundering in the financial system.

5.The Role of Banking Institutions in India

Banking institutions are the first line of defence against financial criminalities in India. Banks are mandated by law to be “reporting entities” under the legal framework of The Prevention of Money Laundering Act, 2002 (PMLA) and stringent regulatory oversight of The Reserve Bank of India (RBI).their role is founded on a complete Anti-Money Laundering (AML) and Counter Terrorism Financing (CFT) ecosystem organized around five core pillars[12]:

[12]Reserve Bank of India, Master Direction – Know Your Customer (KYC) Direction, 2016, RBI/DBR/2015-

Central KYC framework (know your customer).

Banks are strictly employing RBI's master directions on KYC to ensure that illicit funds do not enter the financial network. It includes customer acceptance policy (CAP) which is there to avoid opening anonymous, fictitious or "benami" accounts, customer identification procedures (CIP) which allows identity verification through officially valid documents (OVDs) like Aadhaar, pan, passports and Contemporary onboarding solutions, leveraging strong digital infrastructures such as V-CIP (video-based customer identification process) and e-KYC to authenticate customers remotely and prevent identity impersonation.

Risk classification and management.

Not every customer is a risk in the same way. The banks categorise the clients in various buckets based on risk-based approach (RBA) into low, medium, and high risk. This classification is based on parameters such as geographical location, social/financial status, and the nature of the business. Enhanced due diligence (EDD) is there to access high-risk accounts e.g., politically exposed persons (PEPs), trusts or shell companies, these are subject to intense scrutiny of actual source of wealth and beneficial ownership. Another direction includes sanction screening where the banks screen customer profiles against international and national sanction lists (like the un security council resolutions) to block restricted entities.

Real time transaction monitoring.

Banks have automated AML software to trail transaction patterns and to dot red flags in the money laundering process during the layering and integration stages. They scrutinise for oddly large or intricate cash flows without an economic rationale. The directions strongly recommend employing advanced AML software solutions, which could leverage both artificial intelligence (Ai) and machine learning (ML), for producing alert signals where transactions deviate from the normative pattern, in addition to detecting any possible "money mules" through such accounts. Banks are advised to closely monitor such high-risk business models as multi-level marketing schemes (MLMs), as well as correspondent banking and wire transfers. The document contains a sweeping list of the information required for international as well as domestic wire transfers. There are specific obligations placed on the ordering institution, intermediate institution, and beneficiary institution regarding the information of the

16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 (Feb. 25, 2016, amended as of June 12, 2025).

originator/beneficiary.

Mandatory reporting to financial intelligence unit- India.

A quintessential part of the banking sector's role in stopping money laundering is timely reporting. Suspicious transaction reports (STRs) and Cash transaction reports (CTRs) are two such reports provided by the banks. The banks must make available these reports as required under rule 3 of the PML (maintenance of records) rules to the director of the financial intelligence unit-India (FIU-IND)[13]. Suspicious transactions are those that seem bizarrely complex, lack a valid economic reason, involve suspected criminal proceeds, or could be related to terrorist financing. Not filing it, especially in cases where accounts are later identified as "money mules," is considered non-compliance. All reporting and record maintenance must stay confidential. Banks cannot restrict account operations just because a suspicious transaction report (STR) has been filed. They must not "tip off" customers when suspicion arises. In some cases, where customer due diligence (CDD) could warn the customer, banks should skip further CDD and go straight to filing a STR.

Under separate tax-information exchange frameworks, Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS), banks that are reporting financial institutions must identify and report reportable accounts to the income tax department. This aims to improve transparency of cross-border holdings and reduce chances for laundering through offshore structures.

Record-keeping and evidentiary functions.

Banks play an eminent role in AML enforcement through effective record management.

Banks must keep transaction records, both domestic and international, for at least five years from the transaction date. They also need to keep identification and KYC documents for five years after the business relationship ends. These records must allow for the reconstruction of individual transactions, including nature, amount, date, and parties involved. Identification records, account files, business correspondence, and analytical outputs must be fleetingly available to competent authorities and FIU-IND upon request. This requirement ensures that

[13] Prevention of Money Laundering (Maintenance of Records) Rules, 2005, G.S.R. 436(E), Gazette of India, May 1, 2005.

banks provide a clear trail for investigative and prosecutorial Agencies.

6. Notable cases

6.1 Deputy Director, Directorate of Enforcement v. Axis Bank (2019)[14]

The judgment from the Delhi high court in this case is the key authority on resolving legal disputes between the ED's power to seize property and a bank's right to recover public funds from secured assets. In this case, the ED temporarily attached corporate assets under the PMLA, claiming they were the "proceeds of crime." however, commercial banks had already provided large loans against those same properties, treating them as valid mortgage collateral under the SARFAESI Act. The high court set an important legal limit, ruling that the PMLA does not automatically override the recovery rights of a legitimate secured creditor. The court stated that if a bank gains an interest in a property through a lawful transaction for fair value and conducts proper due diligence without any knowledge of the underlying crime, its right to recover its debt is more important than the state's power to seize.

6.2 State Bank of India v. Directorate of Enforcement (2022) / the reporting entity obligation standard[15]

While previous significant judgments mainly shielded a bank's commercial assets, this case focuses on a bank's structural responsibility as a "reporting entity" under section 12 of the PMLA. This issue arose when the ED penalized a public sector bank for not freezing accounts and promptly reporting suspicious transaction patterns linked to a corporate debtor under investigation for financial fraud. The bank contended that it was waiting for official judicial or police orders before stopping normal banking activities, as freezing accounts suddenly could disrupt legitimate commerce and violate customer agreements.

The court dismissed the bank's defense. It ruled that under the PMLA, banks cannot just be passive bystanders or wait for law enforcement orders to start their compliance procedures. The court stressed that section 12 requires banks to take independent and proactive measures. When a bank notices abnormal, high-volume transactions that do not fit a customer's known

[14] *Deputy Director Directorate of Enforcement v. Axis Bank*, Crl. A. 143/2018 (Delhi H.C. Apr. 2, 2019), Indian Kanoon, https://indiankanoon.org/doc/172990019/.

[15] *State Bank of India v. Deputy Director, Enforcement Directorate*, W.P.(C) 5744/2022 (Delhi HC Mar. 22, 2023) (India), https://indiankanoon.org/doc/113584680/.

economic profile, it must immediately report the activity, start enhanced due diligence (EDD), and submit a suspicious transaction report (STR) to the financial intelligence unit-India (FIU-IND).

7. Challenges and Actionable Reforms in India's AML Framework

Despite strong legislative measures like the prevention of money laundering act (PMLA), several deep-rooted legal, institutional, and structural issues make effective enforcement difficult[16]:

Low conviction rates & judicial gaps:

There is a significant gap between filing a case and acquiring a final conviction. Over 17 years, the ED registered more than 5,400 cases under the PMLA but achieved only 25 convictions. This represents a low-slung conviction rate, extensive delays in procedures and courts, limited resources, and challenges in collecting usable evidence contribute to this problem. Asset recovery and extradition process becomes difficult when high-profile offenders flee the country to escape justice.

Technological lag:

Financial technology is pressing on more quickly than enforcement capabilities. The rapid growth of digital payments and cryptocurrencies adds layers of anonymity that agencies find hard to unknot. They often lack the necessary tools or specialized training to monitor digital transactions effectively.

Vast informal economy & hawala networks:

India's large cash-based informal economy, valued at about $1.2 trillion, along with informal hawala networks, moves an estimated $10 to $15 billion each year entirely outside the regulated banking system. Tax evasion leads to unreported wealth making up around 10–12% of GDP, which creates a constructive environment for mixing illegitimate funds.

[16] Bijay Agarwal, *Decoding Money Laundering: A Comprehensive Analysis of India's Regulatory Framework*, 5 **Ind. J. Legal Rev.** 509, 509–18 (2025).

Fragmented inter-agency coordination:

Not like international systems that share real-time data between financial intelligence units and law enforcement, India's setup suffers from isolated operations. Poor coordination among the ED, FIU-IND, and specific financial regulators slows down investigations.

Reforms to Combat the Challenges

Fixing the conviction gaps and judicial delays:

Setting up dedicated financial tribunals instead of sending complex money laundering cases to regular, overburdened courts, create specialized fast-track tribunals. By having judges trained in forensic accounting, these courts can conduct faster trials and prevent high-profile offenders from taking advantage of lengthy judicial delays. Standardizing digital evidence protocols and to simplify the process for how electronic transaction logs, encrypted messages, and blockchain trails are corroborated for court use. Establishing a clear and updated legal standard for digital data reduces procedural disputes and increases the chances of securing successful convictions.

Overcoming technological gaps:

Deploying automated graph databases instead of trying to track nested shell companies by hand, law enforcement should use network graph software. These tools automatically display corporate structures, showing directors, family connections, and circular payment routes quickly to identify the real beneficial owners behind front companies. Smart contract audits for digital assets to keep up with virtual assets, require non-custodial or decentralized crypto platforms operating in the country to run standardized, audited code. This integrates tracking features at the protocol level, reducing the anonymity criminal's exploit.

Enhancing the agency coordination:

A cooperative and real-time data bionetwork should be maintained to condense barriers between various agencies by building an amalgamated financial intelligence portal. When the financial intelligence unit, tax authorities, and central banking regulators can all see and identify the unusual transaction patterns at the same time, it can help purge the bureaucratic delays and overlapping investigations.

Global cooperation:

It is required to tackle the offenders who flee across borders or hide assets abroad, linking domestic corporate registries with international asset tracking databases becomes the need of the hour. Linking international banking data with shipping invoices helps immediately identify trade-based money laundering (TBML). Therefore, to contend with the offence of money laundering international cooperation is must in the present time. International institutions such as FATF, enables nations to bridge the operational gaps and reduce illicit cross border transactions. Incorporating artificial intelligence and mutual legal assistance treaties (MLA) can help eliminating transnational crimes.

8. Conclusion

The Indian legal and institutional system for anti-money laundering (AML) compliance illustrates that the banking institutions are imperative for handling the financial system. India has a hardy legislative set-up such as the Prevention of Money Laundering Act, 2002, and institutional framework like The Reserve Bank of India and the Financial Intelligence Unit that supervise such regulations. However, countless challenges persist within the system. Impediments that hamper effective AML enforcement hinder the fight against money laundering in India. These include low conviction rates, technological gaps, the presence of informal financial networks, and a lack of coordination among agencies. The expeditious growth of digital banking and new financial products makes it more difficult to detect and prevent illegal financial activities. It is of the essence to make progress on reforms that enhance technology, allow real-time data sharing between agencies, and encourage more international cooperation. To successfully fight against the issue money laundering we need to reinforce our laws and institutions, as well as the proactive stance of banking institutions as the first line of defence. India needs to operate on a system that is heavy on its culture of compliance and innovation to strengthen the resilience of its financial system against money laundering risks and help promote stability and transparency in the global financial system.