

## CHALLENGES AND EMERGING TRENDS IN AML REGULATIONS

**AUTHOR** – HIMANSHI THAKUR, LL.M.(CB&I) STUDENT, AMITY UNIVERSITY, NOIDA, UTTAR PRADESH

**BEST CITATION** – HIMANSHI THAKUR, CHALLENGES AND EMERGING TRENDS IN AML REGULATIONS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (6) OF 2025, PG. 214-219, APIS – 3920 – 0001 & ISSN – 2583-2344.

### ABSTRACT

This study compares the United States and India to examine how anti-money laundering laws are changing with the swift expansion of financial technology. Globally, innovations like decentralized finance (DeFi), fintech platforms, and cryptocurrency are changing the economic environment, but they also increase the possibility of illegal financial behavior. The study looks at how both nations have responded to these issues: the US updated the Bank Secrecy Act (BSA) and put the Anti-Money Laundering Act 2020 (AMLA 2020) into effect, while India expanded the Prevention of Money Laundering Act (PMLA) and introduced a central bank digital currency (CBDC).

In addition, the paper also indicates more and more how AML compliance is a strong complement of technologies, such as artificial intelligence and blockchain. Instead it busies itself understanding the special problems dealt by the non-banking financial companies (NBFC) and also the fintech companies, the e-commerce industry etc. It also urges better horizontal and cross border cooperation for enforcement and the protection of whistleblowers.

The gist of the underlying study concludes that in the epoch of the digitization, the emerging regulatory regime would comprise the risk based, flexible, and coordinated internationally, this state of the play if at all allocates the tradeoff between development of financial innovation and building confidence

### INTRODUCTION

Digital currency represents not just an opportunity, but also a challenge to money laundering, as it has a great impact in the financial system. The difference between fiat currencies and digital currencies lies with the fact that they both function on a decentralized network where their transactions are quicker, more anonymous than fiat currencies. Such an anonymity opened up a weakness that money launderers have been exploiting to conceal illicit proceeds. Digital currencies have regulatory issues in India, as they come outside the traditional financial system that is otherwise regulated under Prevention of Money Laundering Act, 2002 (PMLA). Whereas Section 12 of the PMLA requires financial institutions to keep records of transactions and report suspicious transactions, digital currency

transactions through peer-to-peer (P2P) networks or unregulated exchanges tend to evade reporting.<sup>301</sup>

To consider these threats, the Reserve Bank of India (RBI) has promulgated the idea of the Central Bank Digital Currency (CBDC) by amending the Reserve Bank of India Act, 1934. With better transparency, greater regulatory oversight, the Digital Rupee is issued by the RBI with an aim to provide a state guaranteed substitute of crypto currencies. Digital currencies transactions are now to be conducted under increased vigilance under FEMA, 1999 to curb illicit fund transfer across the border. However, these platforms to trade digital assets away from conventional financial

<sup>301</sup> The Investopedia Team, "Digital Currency Types, Characteristics, Pros & Cons, Future Uses" Investopedia, 3 May 2018.

institutions, or the so called Decentralised Finance (DeFi), are hard to monitor.<sup>302</sup>

And in the US, the transactions of digital currencies have come under the purview of Bank Secrecy Act (BSA), 1970 and Anti Money Laundering Act of 2020 (AMLA 2020). Pursuant 31 U.S.C. § 5318 institutions that are involved in digital assets have to implement CDDs, and report suspicious transactions to the Financial Crimes Enforcement Network (FinCEN). Furthermore, the 31 C.F.R. Part 1010 'Travel Rule' requires that financial institutions collect and exchange information related to each transaction over a specified amount. Nonetheless, international nature of digital currency transactions often means engaging in transactions with offshore institutions who are not subject to U.S. regulations, making compliance with these rules even more difficult.<sup>303</sup>

The USA and India have officially recognized that more solid international cooperation will be necessary to blunt the money laundering risk presented by digital currencies. India has also made AML guidelines compulsory for virtual asset service providers (VASPs) and it is in tandem with the FATF recommendations on combating the practice (AML). Similar, the USA is also actively involved in AML policies worldwide and implementing it globally AML standards of digital currencies. The question in the future will be how to upgrade technological capacities so that digital currency transactions can be traced and monitored without harming financial innovation.

### **CRYPTOCURRENCY AND AML LAWS: INDIA VS. USA**

Enforcing regulations to relate to AML laws and cryptocurrency is perhaps the hardest task due to its decentralized nature and anonymity of involved transactions. Unlike traditional banks,

cryptocurrencies do not fall under the traditional regulatory regime and hence poses to it an impediment for cryptocurrencies to be able to be traced by law enforcement authorities for AML purposes. First, in 2018, banks were banned by the RBI from providing services to crypto businesses based on a circular, which was later overruled by the Supreme Court. Nevertheless, in 2023, the Indian government added something more particularly cryptocurrency transacting through Section 12 of the Act by which VASPs were required to bring in CDD measures too, under the PMLA.

In addition, in the Indian Ministry of Finance, it was suggested that Indian crypto exchanges must register itself under the Companies Act, 2013; and to be liable to fulfil the disclosure obligations under section 90 regarding making their beneficial ownership public. The Securities and Exchange Board of India (SEBI) too has been given supervisory authority over these cryptocurrency exchange platforms, to instill order among them as per rules against money laundering. It is difficult to apply AML rules to the crypto space, however, as cryptocurrency transactions are decentralized and global. Offshore exchange and decentralized finance (DeFi) protocols, private wallet usage, as well as official guarantees and controls on illegal activities cause existing control and regulation to become ineffective.

However, the USA has been more forward in statute to regulate the cryptocurrency under the BSA and AMLA 2020. FinCEN considers cryptocurrency exchanges to be money services businesses (MSBs) under 31 C.F.R. part 1022 and must be registered by FinCEN. Second, they also need to put in place AML programs, carry out CDD and report suspicious transactions. Moreover, under the Travel Rule, cryptocurrency exchanges get to share information of above a certain amount of threshold of a transaction with the aim of preventing illicit blockage of funds. The USA has also exercised stringent sanctions on those cryptocurrency exchanges and individuals who

<sup>302</sup> "Central Bank Digital Currency (CBDC) pilot launched by RBI in retail segment has components based on blockchain technology," available at: <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883> (last visited March 30, 2025).

<sup>303</sup> M. Kendall Day, Stephanie Brooker and Ella Alves Capone, "Anti-Money Laundering Laws and Regulations USA 2024-2025" International Comparative Legal Guides International Business Reports, 6 June 2024.

transact in money laundering using the digital assets.

The difference between India and USA lies in the fact that the cryptocurrency market is being enforced as per AML compliance. Though the USA has had proper policies formulated for cryptocurrency exchanges and has imposed sanctions against those who fail to comply, India has no comprehensive regulation on that front. The RBI has in the meantime introduced the CBDC as a measure to counter the risks associated with private 'cryptocurrencies'. But both countries have common challenges to amass technological tools to monitor blockchain transactions, to regulate offshore crypto exchanges with their international cooperation and to find an equilibrium between innovation and control in the digital asset sector.

### **ROLE OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN IN AML COMPLIANCE**

Today, AML compliance is an important aid to be provided through the use of artificial intelligence (AI) and blockchain technology. By scanning in real time large amounts of financial data, AI based systems can better match the suspicious transaction than conventional tools with their monitoring. In the AML context, financial institutions in India are using the AI powered systems to fulfill their requirements under Section 12 of PMLA. Machine learning algorithms are used in these systems to detect money laundering patterns and generate automatic reports for submitting to the Financial Intelligence Unit-India (FIU-IND). In addition, the Reserve Bank of India (RBI) has introduced AI in fraud detection and AML compliance, integrating the said technologies into the overall financial surveillance system.<sup>304</sup>

The blockchain technology is also increasingly used to increase transparency of financial transactions. For money launderers, blockchain records cannot be tampered with – a quality of

blockchain records that renders them immutable and decentralized. In India, blockchain has been experimented with by Securities and Exchange Board of India (SEBI) to find a way to make all financial transactions transacted without any barrier. On top of that, a government may consider introducing KYC systems based on blockchain to reduce time and costs of the verification process and reduce the risks of identity fraud.

AI based AML system has been extensively used in the Bank's BSA and AMLA 2020 compliance in the United States of America. Banks are required to develop risk based AML programs as per the Section 5318 of 31 U.S.C., and these programs have been made more efficacious with the use of AI technologies. It allows to get immediate risk scoring, anomaly detection and predictive analytics to stop suspicious money laundering operations from happening in real time. In the USA, AI has also been incorporated into the monitoring facilities of FinCEN to be able to monitor suspicious financial activity more efficiently.

The use of blockchain technology in the USA was an important component of AML compliance. It has reduced the risk of failing customer due diligence (CDD) as per the current regulatory standards to which financial institutions are obliged to adhere. In addition, the USA has promoted secure cross border payment using blockchain in order to combat illicit cross border money transfer via traditional banking system. At the same time, the acceptance of blockchain supported financial services, such as smart contracts as well as DeFi, has been able to reduce the risks of money laundering associated with new technologies in the financial industry.

Both India and USA share that they see promise of AI and blockchain in making AML enforcement more effective. However, there are still problems in ensuring that AI is used in almost ethically way possible and also with overcoming data privacy problems and creating regulation that can be brought into

<sup>304</sup> "Leveraging AI in Suspicious Activity Reporting," Flagright *available at*: <https://www.flagright.com/post/leveraging-ai-in-suspicious-activity-reporting> (last visited March 30, 2025).

compliance with financial financial systems. In the future, both nations need to concentrate on developing stronger regulatory cooperation, putting money into AI-based compliance solutions, and having standard blockchain protocols to bring a better and more secure financial system to the world.

### **STRENGTHENING AML FRAMEWORKS FOR NON-BANKING FINANCIAL INSTITUTIONS (NBFCs)**

Non-Banking Financial Institutions (NBFCs) contribute significantly to the financial system in the form of extending credit and other financial products to firms as well as individuals. Because they enjoy a more lenient regulation than regular banks, they also have emerged as a potential entry point for money laundering. The Reserve Bank of India Act, 1934 has been used to place NBFCs and coverage under Prevention of Money Laundering Act, 2002 (PMLA) have been some measures undertaken in India to comply with AML guidelines. NBFCs are asked to adopt Know Your Customer (KYC) norms and to maintain transaction records under Section 12 of the PMLA. RBI's Master Direction on KYC in turn gives detailed norms to prevent financial crimes to the NBFCs.<sup>305</sup>

Despite these regulations, though, there are a couple of hurdles in mandating AML measures in NBFCs. As NBFCs differ from the housing finance companies to microfinance institutions, the main concern is the heterogeneity of NBFCs, and uniform enforcement becomes difficult. A majority of NBFCs, however, do not have a strong compliance infrastructure and technological ability to make this [suspicious transactions] identification. Moreover, there is a considerable involvement of NBFCs in providing loans to small enterprises and rural clientele and agreements for money transactions not cushioned with documentation increase easy chances of money laundering. Stepped up supervision, stringent compliance measures, and moving towards AI based transaction

monitoring techniques for better detection purposes are some of the ways by which AML procedures of NBFC are reinforced.

In the USA, these AML rules for NBFCs fall under Bank Secrecy Act and Anti Money Laundering Act of 2020 (AMLA 2020). NBFCs, like financial institutions, are required to set up an AML compliance program and file Suspicious Activity Reports with the Financial Crimes Enforcement Network (FinCEN) pursuant to 31 U.S.C. § 5318. The USA PATRIOT Act also requires increased due diligence on high risk customers and transactions. Whereas in India, the RBI primarily monitors compliance to the AML regulations with respect to NBFC, the USA has several regulatory agencies like FinCEN, Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) which oversee compliance to AML regulations of the USA. The combination of multiple regulators can produce higher regulations, however, at the expense of regulation complexity.

In order to consolidate AML measures for NBFCs, both India and the USA must move towards a risk-based system wherein entities of greater risk are treated with greater restrictions. Cross-border collaboration is also necessary since NBFCs may conduct foreign exchange transactions that are susceptible to exploitation for money laundering. Increased technology adoption, enforcement of penalties against non-compliance, and regulatory convergence with international best practices in AML, like the Financial Action Task Force (FATF) guidelines, are needed to strengthen AML regulation in the NBFC space.

### **AML CHALLENGES IN THE FINTECH AND E-COMMERCE SECTOR**

With the frantic development of the fintech and e-commerce industries, AML enforcement faces new challenges. Since Fintechs like digital payment operators, online lending platforms and cryptocurrency exchanges do work outside the conventional banking channels, it becomes more challenging for Fintechs to be compliance

<sup>305</sup> "Reserve Bank of India," available at: <https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=1167> (last visited March 30, 2025).

oriented towards AML. Under the PMLA and hence KYC and CDD, fintechs in India are governed by Section 12 of the Act. Additionally, RBI has directed that the digital lending platforms and payment service providers are AML compliant. However, the number of transactions as well as pace of digital payments makes it a challenging thing to identify suspicious activities in.

Financial transactions as well as cross border remittances are also possible through online routes, which is something that paints the face of e-commerce in the same mould of possible risk. As for the risk of money laundering, fictitious transactions, misuse of electronic wallets, and shell companies that operate on the online e-commerce space may lead to the same. Information Technology Act, 2000, and Foreign Exchange Management Act, 1999 (FEMA) respectively have been imposed on online payment gateways, and e-commerce industry to report the remittance made above some high sums. However, there are enforcement gaps because we do not have a centralised monitoring watch on e-commerce AML controls.<sup>306</sup>

In the USA, the AML regulations of the BSA and AMLA 2020 and the FinCEN Travel Rule are followed in the contexts of e-commerce platforms and fintech companies. For companies such as digital payment companies, risk based AML programs and above the threshold reports (over 31 C.F.R. Part 1010) are mandated by law. However, just like India, the USA is not able to monitor illicit digital payments in a P2P mode and in DeFi platforms.

To take on the AML threats in fintech and e-commerce, India and the USA need to either make the regulatory regime in both countries more effective to cover up new financial technologies, or develop a central regulatory regime that serves both for them. Thus, it would necessitate deployment of AI based transaction

monitoring systems alongside more transparent guidelines for FinTech startups regarding AML and close global cooperation on preventing cross border money laundering via digital platforms. Regulators also have to have a good cooperation working with the private sector in a manner consistent with the AML controls, as well as with remaining strong supervision over electronic transactions.

### **STRENGTHENING WHISTLEBLOWER PROTECTIONS IN AML ENFORCEMENT**

AML Compliance is dependent on Whistleblowers for the reason that they inform the suspicious finances and expose systemic vulnerabilities of financial institutions. However, whistleblower demotivation threatens the AML regimes' effectiveness because of lack of whistleblower protections. The Whistle Blowers Protection Act, 2014 is the law currently in place in India with all such reporting exposed as no longer protected there. However this has been blamed on the absence of strong enforcement powers and no incentives for whistleblowers. This unwillingness on the part of the government to set up an AML whistleblower program under the PMLA has also caused a vacuum which has led to financial crime reporting gaps.<sup>307</sup>

The AML enforcement in India should enhance the whistleblower protection by modifying the existing framework for assuring greater legal safeguard, economic benefit and anonymity to the parties who channelize money laundering operations. Stimulating the reporting of suspicious transactions by a greater number of people without risking reprisals would arise from granting autonomy to an AML whistleblower agency at the Financial Intelligence Unit-India (FIU IND).

In a contrast, the USA has better whistleblowers protection scheme under Dodd Frank Wall Street Reform and Consumer Protection Act and 2022 AML Whistleblower Improvement Act.

<sup>306</sup> "Clean Money is a Click Away: The Money Laundering Risks of E-Commerce," Protiviti available at: <https://www.protiviti.com/hk-en/whitepaper/clean-money-click-away-money-laundering-risks-e-commerce> (last visited March 30, 2025).

<sup>307</sup> stefano, "AML Whistleblower Protection: An Essential Tool Against Financial Crime" relycomply, 2023 available at: <https://relycomply.com/aml-whistleblower-protection/> (last visited March 30, 2025).

Under 31 U.S.C. § 5323, whistleblowers are entitled to monetary rewards and protection from legal recourse for being retaliated against in response to reporting information that leads to effective AML enforcement actions. FinCEN administers the whistleblower program with its incumbent confidentiality protocols for protectors. However, AML enforcement has tightened in the financial system following material revelations of the abuse of the system, culminating in financial revelations.

The USA provides it with an example to follow: creating a similar reward and punishment system for the whistleblowers in the AML space. If AML can be enforced by offering financial rewards to AML whistleblowers and maintaining confidentiality and strong penalties to retaliate against AML informants, it should be more effective. When it comes to cross border whistleblower arrangements, there must be cooperation between the two of these nations, people must be able to report the money laundering enterprises of multinational financial institutions.

### **CONCLUSION**

The speed of technological innovation in the financial world, with all the forces, including cryptocurrencies, fintech apps, decentralized finance or Decifi, places a strain on AML regulations around the world. India and the United States are facing similar problem of having to keep up with these rapid growing innovations while safeguarding the independence of its financial system. The India example, for one thing, has gone a long way to raising digital currency transactions to prevent money laundering by putting digital currency transactions under the Prevention of Money Laundering Act (PMLA) and introduce Central Bank Digital Currency (CBDC) as part of its efforts to increase transparency. However, the U.S. has made the most headway in its further advancement of legal frameworks including the Bank Secrecy Act (BSA) and the AMLA 2020, so that it may deal more directly with the problems presented by crypto.

The new technologies, such as artificial intelligence and blockchain are beginning to bear a big part in AML efforts. Among among others, they are providing tools for real time monitoring, spot suspicious pattern and make transaction records secure and tamper proof. But tech alone isn't enough. While many countries may need to update their laws, and there is much international cooperation work to be done, still countries need to help financial institutions develop the skills for the management of risks associated with cross border, anonymous transactions.

Money laundering is especially rampant in sectors like NBFCs, fintech startups and the likes, and makes it important for more thorough oversight and smarter compliance systems on the basis of risk and consistent regulation in the sector. Financial crime is also important work of the whistleblowers. However, protections for whistleblowers in India are actually still quite weak—to the point that it is tougher to bring wrongdoing to light, as in the U.S.

Going forward, India and U.S. have to create an environment to accommodate innovation while keeping in AML standards intact. To handle money laundering in this modern day global and digital world, most importantly, it will be beneficial to strengthen global partnership, to invest in new tech infrastructure, and align national policies and guidelines under international standards such as those from the FATF.