Emerging Frontiers in KYC and AML Compliance[1]

The award for the oldest and most famous acronym-twins for bankers could possibly go to KYC (Know Your Customer) and AML (Anti Money Laundering), despite increasing number of siblings such as CFT (Counter Terrorist Financing) and CPF (Counter Proliferation Financing) having been added to the compliance specie. They are not identical twins to be mixed up either. Despite being often treated as a pure procedural matter, they are bedrocks for safeguarding the integrity of the financial system, equally protecting the banks as well as its customers. To take a look at the life of this celebrated acronym, the first circular on KYC/ AML, without using the terms, was issued by RBI on August 12, 1976, in the context of issue of DDs/TTs in excess of ₹5,000 and the second circular on November 11, 1987, in the context of frauds in opening new accounts. The Financial Action Task Force (FATF), the global standard setting forum, was founded in 1989. The word KYC was first used in an RBI circular of December 5, 2001, in its communication to banks regarding implementation of Prevention of Terrorism Ordinance, 2001. The Prevention of Money Laundering Act, 2002 (PMLA) was enacted in India on January 17, 2003. Ever since, the subject matter has never paused in presenting dynamic trends and challenges to financial service providers, particularly banks. In the train of the first full-scale Mutual Evaluation (ME) of India by an FATF team concluded last month, its rather timely to look at the emerging frontiers in KYC and AML compliance for a better course correction and future preparation strategy.

2. Before proceeding to enumerate the frontier challenges, let me preface it with a few recent learnings, in opposite ends of the twain. (a) There are much more nuances and granularities to the KYC/AML directions and effectiveness of its implementation as learned during recent time when all of us collectively prepared to go through the FATF assessment. There may be a need to be more explicitly alert to counter terrorism finance (CFT) in the present scheme of things, (b) Regulated Entities need to be much more responsible and discreet in communication and dealings with customers while applying different levels of due diligence. Disclosures about risk categorization along with reasons and internal procedures / polices not only violates the extant regulatory

[1] Keynote address by Jayant Kumar Dash, Executive Director at CAFRAL Virtual Program on KYC and AML on December 8, 2023.

guidelines in the matter, but it also potentially creates a backlash effect affecting the intents of the very technicalities. Minding the respects that most customers of the bank deserve, while not flinching on the diligence that is required, is not a small challenge or skill that bankers must learn.

3. In this context, a few recent amendments to the KYC/AML rules In October 2023 that may need careful treading for implementation. First, the definition for Customer Due Diligence now requires use of reliable and independent sources of identification for customer or beneficial owner. Secondly, the ongoing due diligence for transactions in a customer's account conform not only to business and risk profile of the customer but also to the source of funds and wealth (SOF/SOW). Thirdly, the onus of updating of any documents submitted to an RE for account-based relations has now been shifted to the customers and it has to be done by them withing 30 days of any updating of the said document at the origin end. The challenges in implementing these changes, along with others, are things which many REs are yet to give due attention to.

(Explainer: There could be some overlaps between SOF and SOW. For example, a person's SOF and SOW could both be attributed to employment income. The key difference is the depth of the investigation and whether the interest is in the money being used or in the individual making the purchase. SOF is a "moment in time" analysis in a transactional context, while SOW considers the stock of funds accumulated over a time horizon)

4. With multiple laws and rules assuming more granularity, cross-cutting at times, and casting progressively higher burden of compliance related to various financial crimes and routing of crime proceeds on the regulated financial service providers, particularly banks, has to be seen in a larger canvass of a fast growing and innovating financial system as well as superior expectations from the banks. The reasons why I mention it here is for the boards of such financial entities be spurred to rethink the entire KYC/AML monitoring and compliance architecture to remain on the efficient frontier. Looking at various challenges and costs involved in such a cumulative approach, RBI as well as Government of India are also fully alive to system level infrastructure and processes that could minimize multiplication of efforts for both financial service customers as well as the regulated entities.

Now, let me try to capture certain trends and emerging frontiers in the space of KYC/AML compliance world over from which India may not remain immune for long. These trends would present their own challenges for Regulated Entities in India while creating an efficient system design.

Rapid changes and increasingly stringent regulations

5. The easiest thing to predict about future of KYC/AML compliance is that the requirements are and will be undergoing rapid changes and may become progressively more stringent, granular and demanding. These changes will be essentially driven by the constant changes taking place in the threat landscape of financial crimes and the developments in regulatory landscape. As financial institutions crack down, bad actors will always find newer ways to commit financial crimes. Law enforcement agencies have a hawk's eye on facilitators of money laundering, including professional money launderers and complicit financial institutions. By way of trade-off between investment in KYC/AML compliance and the cost of non-compliance, probably the latter would hang heavier. In most KYC/AML breaches, after-event attribution of compliance failure with the benefit of hindsight may prove to be an costly and indefensible affair to an institution or individual executive/s, as seen in some recent cases. The ex-ante assessment by auditors or supervisors, therefore, should be given due weightage. Secondly, as international rules of engagement are often principle based, setting a modular practice and highly configurable / scalable architecture that accounts for domestic / international guidelines may be a balanced approach.

Perpetual KYC (pKYC)

6. Perpetual KYC signifies a paradigm upgrade of the conventional KYC practices. Unlike traditional KYC, which typically involves initial and thereafter, scheduled or interval-based customer reviews, pKYC ensures that customer data is continuously monitored and validated, thereby maintaining its accuracy and relevance in the ever-evolving financial landscape. Usually, pKYC requires implementing automated systems and processes typically powered by data analytics / artificial intelligence (AI) and machine learning (ML). This continuous scrutiny enables financial institutions to

swiftly identify and respond to anomalies or risks on nearly real time, ensuring that the customer profiles are always up-to-date and compliant with regulatory norms. pKYC has emerged as a response to the increasing complexities and challenges in the global financial landscape. As financial crimes become sophisticated and regulations become stricter, pKYC serves well to customer verification, ensuring that financial institutions stay ahead in compliance and risk mitigation. Some of the global banks also follow social data enrichment model to flag or smell potential financial crime.

7. However, certain industry best practices for pKYC that may have to be weighed in include (i) sound data management, provenance and governance practices (ii) explainability for both overall function as well as individual outcomes, keeping in view the regulators' antipathy for black box solutions; (iii) complete awareness and mitigation of the residual risks associated with emergent technologies; (iv) right balance between automation technologies and human oversight, and (v) establishing a dynamic 'digital profile' of customer incorporating relevant, auditable and up-to-date information used for pKYC processes. Upgrading to pKYC and use of modern technologies may become a *de rigueur* for financial institutions in coming time, as it elevates the level of AML compliance, provides better protection from reputational risks, helps operational cost minimization, enhances efficiencies, better utilises human effort, and ensures that a financial institution maintains above par industry standards.

8. Typical AML transaction monitoring technology solutions are often unconfigurable to the underlying risk strategies of their banking users. Taking a holistic approach to automated KYC with a single-pane-of-glass view of compliance risks and business metrics needs an integrable solution. Afterall, financial crime risk can manifest in ways beyond the thresholds of compliance and regulatory risk. Banks are increasingly treating anti-financial crime strategies as crucial initiatives within their operational risk programs, to tackle several challenges, including counterparty risk, reputational risk and other emerging risk associated with the ethical impacts of financial crime. In this context, convergence of risk assessment/intelligence and core transaction monitoring systems assumes some criticality.

Integrated approach to Sanction Screening

9. As there is increasing geo-political events all around and India is bound to be aligned to certain values keeping the broader national interest in view, there could be increased global attention on how we implement sanction screening processes. Basic and standalone reliance on customer screening and transaction filtering may not prove to be adequate from effectiveness points of view, as potential structures are created around many sanction-defying transactions. That warrants convergence of sanctions programs with AML & KYC programs enabling identification of trade sanction circumvention for desired effectiveness. Screening payments for direct links to blacklisted parties may miss signs of evasion attempts to conceal the ultimate destinations and users of prohibited goods. Continued siloisation of AML/CFT and sanctions functions at some banks can lead to unwittingly, or inadvertently, processing payments for controlled goods and involving designated entities.

10. That underlines another reason for banks to consider a holistic compliance architecture across screening processes. This requires interconnectivity between inherent customer / other party risks with AML processes to prompt investigations that can capture sanctions evasion schemes. Right mix of solutions supplemented by cross-training between sanctions and AML analysis is necessary to support these efforts and drive efficiency. AI embedded in many solutions can play transformational role in leveraging processes with data and intelligence to produce better outcomes for risk mitigation.

AI Maturity in AML/KYC Technology

11. Most *avant garde* KYC and AML solutions offer artificial intelligence (AI) and machine learning (ML) to optimize operations by enabling transaction-monitoring to proactively address potential fraud / financial crime cases. Use of AI can help banks deal with a number of exposures that come packaged with digitalization. It can lighten the need for human intervention at each stage in the context of circumstances requiring the prevention of money laundering. Although AI can never be able to fully replace human intelligence, it can help to reduce the need for human authorization and speed up various aspects of AML by working on both Type I and Type II errors.

12. Typical client screening tools used by banks in their AML processes are generally driven by pre-observed red flags and statistical approaches for transaction monitoring. However, with these tools, false positives abound, accounting for nearly 50 % of AML alerts and costing banks dear to resolve through resource deployment if they choose to be diligent. Advanced ML/AI algorithms should be capable of analyzing large amounts of data quickly with their pre-trained intelligence, detect fraud with improved accuracy, and analyze alerts faster. This is expected to eliminate good amount of manual and tedious routine or base-level tasks. ML/AI can also be made capable of capturing the latest trends, modus operandi and behaviors in ML activities and parametrize those. This will require training and testing of AI models on high-quality data and reliable outcomes; putting in place mechanisms to monitor and supervise the performance of AI models and establish procedures for addressing errors and biases. You will be glad to learn that RBI Innovation Hub is now working with a cohort on KYC/AML area (e.g Face recognition technology) to help the system adopt more acceptable advanced technology.

Increased Focus on Ultimate Beneficial Ownership (UBO)

13. Of late, more transparent UBO laws have been a worldwide trend, including in India, towards greater transparency. In the USA, the publication of FinCEN's proposed rule for the application of the Corporate Transparency Act's Beneficial Ownership criteria, effective from 2024, is only a sign of this trend. The final rule urges certain firms registered to do business in the US to reveal recognizing and Beneficial Ownership Information (BOI) to the US federal government. By providing more openness and information about the legitimate owner of the company, the risk of financial crime is targeted to be contained. Nevertheless, not all countries, such as Switzerland, may join the bandwagon, which could create chinks in anti-money laundering armors. In UK, the passing of the UK's Economic Crime (Transparency and Enforcement) Act came into force in March 2022 and represented a clear shift in UBO space. The Act includes reform to Companies House as well to provide a clear view of companies and legal entities created within the UK. The reforms include identity verification for new and existing company directors / PSCs (Person with Significant Control). This new law also envisages creation of a new public Register of Overseas Entities, which will enable disclosing of UBOs who own UK property through non-UK

entities. Another event related to UBOs in Europe influencing future roadmap is the recent ruling by the European Courts of Justice (ECJ), invalidating a provision contained in the EU 5th MLD (Money Laundering Directive) that guaranteed public access to information on companies' real owners. Each initiative may, albeit, come with its share of criticism.

14. In India, you would have noticed recent amendments to definition of Beneficial Ownership (BO) for different forms of entities. While the FATF recommendations do talk of a BO Registry, the Indian solution to it should be on its way in days to come. Globally, the lack of public access to such BO Registries raises the risk of data theft victims who can now not verify if their identities being used to construct false entities involved in financial crime, with good number of instances in India. Registers generally being accessible to governments and their agencies, it remains a challenge for law enforcement alone to ensure adequate monitoring with limited resources. It may be challenging to determine the actual ownership of assets held in complex ownership structures like shell companies and offshore bank accounts / overseas 'box' companies. Despite the importance of UBO identification to AML compliance, the difficulty arising from absence of a standardized regulatory framework and a comprehensive worldwide database will form challenges in coming days.

Know your Business (KYB)

15. KYB is often viewed as an extension of Know Your Customer (KYC) norms; the reason being young age of KYB regulation. While KYC procedures have been cast for decades, businesses were not subjected to the same level of diligence until recently, allowing perpetrators of financial crimes to exploit corporate veils for illicit activities. KYB, also known as corporate KYC, is the process of verification by one business that another business it deals with is legitimate and safe to do business with. The salient difference is that KYB focuses on the business's owners, shareholders, and suppliers before considering customers or consumers. The focus is mainly on identifying the Ultimate Beneficial Owners (UBOs), or the key individuals behind the business, to understand who benefits from the business's financial transactions and how, directly or indirectly. Continuous AML monitoring throughout the business relationship would follow such identification. In Europe, regulators corrected the legal blind spot by specifying KYB in the 4th AML Directive released in 2017. The updated

regulation came a year after US Financial Crimes Enforcement Network (FinCEN) included KYB rules in Customer Due Diligence Requirements for Financial Institutions.

Cross Border Payments / Trade Based Money Laundering

16. The globalization of financial services and resultant AML challenges has put the spotlight on cross-border payment transactions on the face of varying legal constraints, and complex ownership arrangements. Identification and Investigation of possible money laundering situations is further complicated by the growing difficulty of tracking cross-border payments as business becomes increasingly globalized and the cross-border payment innovations are moving to the next phase. QR code-based systems that allow for cross-border interoperability above *de minimis* have gained traction in many regions, particularly in Southeast Asia. Announcement of a number of new QR code-based corridors in recent days are signs of future of this mode. The challenges of service or subscription payment remittances or P2P transfers camouflaging ML transactions need special skills to detect. Trade-based ML schemes are becoming more sophisticated. Detecting and preventing these complex transactions, which involve the use of international trade, poses a dainting challenge for AML efforts of banks. The possibility of progressing from a local to global KYC framework may not be just an imagination with potential integration of domestic national identity systems with select foreign jurisdictions are being explored.

Virtual Digital Assets

17. Globally speaking, cryptos are becoming more regulated all over or regulation being demanded. Recent events involving FTX and Binance in the USA are phenomena foretold by Governor of RBI long ago. Enhanced crypto regulations will be one of the AML trends to look out for in 2024. The anonymity that accompanies cryptocurrency has made it easier than ever for scammers and criminals to transfer large funds without getting tracked or noticed. Most authorities have not simply banned businesses associated with cryptocurrencies for obvious reasons; instead, they claim to be taking a risk-based, tailored approach to regulating the industry in order to avoid strangling innovation. Cryptocurrencies attract money launderers and other criminals to take advantage of inconsistent regulatory norms among jurisdictions. It has been

reported that hackers have stolen cryptocurrency worth $4.3 billion between January and November 2022 representing an YOY increase of 37%. Thus, it will be fair for banks to expect tighter crypto laws in 2024. If you are wondering what is in for us in India, the answer lies here: when crypto related reporting entities report suspicious transactions or those related to financial crimes to Indian authorities, it is likely that one of the legs would have passed through banking system and lack of due diligence can be called out. Crypto related market infrastructure in India, located off-shore (catering to Indian clientele) have been made REs (reporting entities) under PMLA.

Designated Non-Financial Business and Profession (DNFBP) reporting

18. Though it might have escaped the notice of the bankers, more and more non-financial entities who may have sharing surfaces with some stage of money laundering are being designated as DNFBPs in India. Very recently in UK, A British lawyer has been convicted of 'tipping off' a client about a money laundering investigation in the first-ever case of its kind, according to the Serious Fraud Office (SFO). When the SFO requested information from the solicitor about the purchase of a £8m property by his client, he tipped him off about it. As indicated in the previous point, the risks for banks with such increasing reporting sources from outside, any slack in due diligence in the account maintaining bank would be more likely to be detected. That also flags the issue about how the operating staff deal with the alerts / STRs while involving clients.

Transaction Laundering:

19. Transaction laundering occurs when an approved merchant processes payment transactions on behalf of another entity, unknown to the merchant acquirer or payment provider. This, as per literature, can typically include (a) Front companies i.e functional companies intended to disguise and obscure illegitimate financial activities; (b) Pass-through companies i.e legitimate companies that *bona fide* goods or services but are either constrained to process unrelated transactions through their merchant accounts and (c) Funnel accounts i.e legitimate businesses that unknowingly enter illicit transactions into the network payment system. While the burden of caution may be more on account aggregation service providers, the vigilance of banks come into play when the accounts of receiver of such laundered money is maintained with them. Of

late, there are signs that some FinTechs effectively act as payment aggregator without valid authorization and operation of their bank accounts would pose a risk to the banks.

KYC/AML Compliance in Embedded Finance

20. Embedded Finance, integrating financial services into non-financial products and services, is one of the growing trends in the social media / e-commerce space. While providing customers with new age convenient access to banking and payment services, it also presents significant compliance challenges to banks. For banks, the challenge lies in integrating AML/KYC solutions by the front-end entities/ systems using embedded financial services This requires front-end businesses to have a comprehensive compliance program including policies, procedures, and technology solutions after conducting assessment to identify potential risks.

ML/TF Vulnerabilities Associated with Cultural Objects and the Market[i]

21. There could be a dark side to art. The trade in art, antiquities and other cultural objects is a billion-dollar industry. The typical market participants are dealers in cultural objects, auction houses and storage facilities. The ML typologies involving art and other cultural objects include using them as a vehicle to transfer or hide illicit proceeds, use of cash in transactions, misuse of legal persons / arrangements and intermediaries, use of under or over pricing or fictitious sales and fake auctions. Terrorist financing is another risk for those working predominantly in the markets for cultural objects. It was reported that Islamic State of Iraq and Levant (ISIL) notoriously pillaged important archaeological sites in Syria and Iraq, and used sales proceeds and taxes levied on diggers to generate funds. This can be extended to market for digital art and NFTs. Identifying the market participants in this ecosystem is the key challenge. We have good number instances in India to quote as well.

Countering Ransomware Financing[ii]

22. The global scale of financial flows related to ransomware attacks has grown dramatically in recent years. A ransomware attack is a form of extortion and the FATF Standards require that it be criminalized as a predicate offence for money laundering. This report finds that payments and subsequent laundering of ransomware proceeds

are almost exclusively conducted through virtual assets. Ransomware criminals exploit the international nature of virtual assets to facilitate large-scale, nearly instantaneous cross-border transactions, sometimes without the involvement of traditional financial institutions that have anti-money laundering and counter terrorist financing (AML/CFT) programs. Criminals further complicate their transactions by using anonymity-enhancing technologies, techniques, and tokens in the laundering process, such as anonymity enhanced cryptocurrencies and mixers. The bankers would be challenged if any leg of such transactions touch their shore.

Crowd Funding for Terrorism Financing[iii]

23. Although the majority of crowdfunding activity is legitimate, Financial Action Task Force (FATF) research has shown that the certain religious extremist groups and ethnically or racially motivated terrorist individuals and groups have exploited it to raise money for terrorist financing (TF) purposes. the definition of crowdfunding covers formal crowdfunding platforms and crowdfunding activities on social media, messaging applications or other dedicated websites. It also considers hybrid means of crowdfunding that combine digital and physical fundraising. This threat has critical applicability to Indian situations as well. Banks are inevitably a party to this as it happens generally through banks accounts.

Crime as a Service (CaaS)

24. The service models are no more limited to software or clouds and has expanded to spaces in money laundering. CaaS model is one where an expert cybercriminal sells or rent their advanced tools or services to other, often lesser-endowed cyber criminals. In a way, cybercrime gets commoditised through CaaS. Well-funded cyber professionals remain unregulated and ungoverned but well-co-ordinated / networked for ML activities by adopting certain business models. As with any other business, they take advantage of new ways by leveraging technology to maximize efficiencies and gains while minimizing traceability and streamlining costs. Banks would definitely come into picture when the crime proceeds reach integration stage.

Conclusion

25. Staying ahead of evolving trends and addressing the challenges in both KYC and AML will always be an ongoing endeavour for banks and financial institutions. These areas are vital for preserving financial integrity and security, and hence merit continuous adaptation and innovation to tackle new threats. The regulatory landscape is bound to grow complex and constantly evolving, demanding significant resources from banks for its alignment and realignment. The disconnect between works of KYC/AML teams and the business functions of the bank needs to be bridged to strike a right balance. While culture can be slow to change, technology and structured processes can help in the interregnum. It will not be an overstatement, to say that there may be need to reimagine KYC/AML architecture de novo or transforming KYC into a profit centre or competitive advantage through right integration of KYC/AML into the overall risk management systems and customer lifecycles. Hence, the importance of pushing the current state of KYC/AML risk management beyond the visible the frontiers cannot be relegated to a future anymore.

I wish the deliberations during the rest of the day to be productive and useful to the participants.

Thank You.

xx**xx

[i] FATF Report – Money Laundering and Terrorist Financing in the Arts and Antique Market, February 2023
[ii] FATF Report – Countering Ransomware Financing, March 2023
[iii] FATF Report – Crowd Funding for Terrorism Financing, October 2023