INDIAN BANKS' ASSOCIATION

WORKING GROUP

Draft Framework

To protect the Interest of End Users from the Menace of Money Mule Accounts

January 2025

Members of the Working Group

Name of the Member	Institution
K Srinivasa Rao	Indian Banks' Association
Aayushi Parnami	A U Small Finance Bank
Suresh Singh Rathore	AU small Finance Bank
Saurabh Maheshwari	Axis Bank
Suraj Mehta	Axis Bank
Sanjeev Jaiswal	Axis Bank
Ravi Boddu	Bank of Baroda
Rajiv Kumar Mishra	Bank of Baroda
P Chakkaravarthy	Canara Bank
P Anup Kumar	Central Bank of India
Naveen Janardhan	HDFC Bank
P Vinodhkumar	HSBC Bank
Rajesh Kumar	Punjab National Bank
Amresh Prasad	Punjab National Bank
Jayesh Kadam	Standard Chartered Bank
Akhilesh Pandey	Standard Chartered Bank
Jairam Manglani	Standard Chartered Bank
Mukesh Kumar Dhama	State bank of India
Harish S. V.	State Bank of India
Tata Venkat Venugopal	Union Bank of India
Gururajan S	YES Bank
Rajat Taneja	YES Bank
Selvin Rajendran	YES Bank

CONTENTS

Index	Page
1. Background	06
2. Current Regulatory Guidelines	06
2.1 Prevention of Money Laundering Act (PMLA, 2002)	06
2.2 Reserve Bank of India (RBI) Guidelines	06
2.3 FATF Recommendations	07
2.4 FIU-IND Guidelines	07
2.5 Indian Cybercrime Coordination Centre (I4C) Guidelines	07
2.6 International Standards	08
3. Current Mechanisms to Tackle Money Mule Accounts	08
3.1 Know Your Customer (KYC) and Customer Due Diligence (CDD)	08
3.2 Transaction Monitoring Systems (TMS)	08
3.3 Suspicious Transaction Reporting (STR)	08
3.4 Sanctions Screening	09
3.5 Cross-border Transaction Alerts	09
3.6 Placing debit freeze / Hold on account	09
4. Challenges in Current Mechanisms	09
4.1 High False Positives	09
4.2 Latency in Detection	09
4.3 Limited Data Integration	09
4.4 Adaptation by Criminals	10
4.5 Resource Constraints	10
5. Proposed Mechanism Using Data Driven Detection Systems	10
5.1 Data Enrichment	11
5.2 Behavioural Analytics	11
5.3 Anomaly Detection Models	11

5.4 Real-time Monitoring 12
5.5 Network Analysis 12
5.6 Explainability of Models 12
6. Pre-onboarding checks 13
6.1 Pre-onboarding – KYC & Due Diligence checks 14
6.2 Digital onboarding checks suggested for effective screening 14
6.3 Validation of OVDs 16
6.4 Controls pertaining to location/distance 18
6.5 Initial funding related controls 18
6.6 Due diligence measures using Tech enablers 18
7. Post-onboarding checks / monitoring 19
8. Portfolio monitoring 22
8.1 Data Collection and Integration 22
8.2 Baseline and Risk Profiling 23
8.3 Monitoring and Detection 24
8.4 Investigation and Reporting 24
9. Transaction Monitoring, Trigger Basis Alternate Data Feed (NPCI / NCRP) 24
10. Real time sharing of fraudulent transactions data between banks 27
11. Expectations from Banks 27
11.1 Investment in Technology 27
11.2 Staff Training 27
11.3 Collaboration and Information Sharing 27
11.4 Adherence to Regulatory Standards 28
11.5 Periodic Audits and Assessments 28
12. Role of Law Enforcement Agencies 28
12.1 Collaboration with Financial Institutions 28
12.2 Use of Advanced Technology 28
12.3 Training and Awareness 28
12.4 Cross-border Cooperation 28
13. Expected Benefits 28

13.1 Enhanced Accuracy 28
13.2 Proactive Detection 29
13.3 Resource Optimization 29
13.4 Scalability 29
13.5 Improved Regulatory Compliance 29
14. Conclusion 29
15. Abbreviations 29
16. Suggestions 31
17. ANNEXURE-I: Use-Cases by Punjab National Bank 33
18. ANNEXURE-II: Case-study by Union Bank of India 38

Considering the varying levels of preparedness and automation, the Committee was of the opinion to create a framework which prescribes minimum standards that needs to be adhered to by every bank. Each of the Banks may use this framework as a guide to build upon their own systems/solutions to monitor compliance according to their own needs.

1. Background

Money laundering remains one of the most significant threats to financial ecosystems worldwide. Among the tools employed by criminals, money mule accounts play a critical role in disguising the origins of illicit funds. These accounts are often used by individuals who knowingly or unknowingly facilitate the movement of money acquired through fraud, hacking, or other illegal activities like drug and human trafficking.

Money mule accounts are typically characterized by unusual transaction patterns, such as frequent international transfers, unusually high number of counterparties, high velocity transactions, sudden spikes in activity, or transactions inconsistent with the account holder's profile. Despite efforts to curb this activity, the rapid adaptation of techniques by criminals and limitations in existing monitoring systems necessitate a more robust and dynamic framework. This document proposes an enhanced framework, leveraging advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML), while also outlining expectations from banks to ensure effective implementation.

---

2. Current Regulatory Guidelines

Several regulatory guidelines and frameworks have been established to tackle the misuse of accounts as money mules. These include:

2.1 Prevention of Money Laundering Act (PMLA, 2002)

The PMLA provides the foundational framework for combating money laundering in India. It mandates stringent Know Your Customer (KYC) and Customer Due Diligence (CDD) measures, the retention of records, and the timely reporting of suspicious transactions to the Financial Intelligence Unit of India (FIU-IND).

2.2 Reserve Bank of India (RBI) Guidelines

The RBI has issued a series of circulars under the Master Directions on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards. Key provisions include:

- Continuous transaction monitoring using technology-enabled solutions.
- Periodic risk assessments based on customer profiles.
- Identification and reporting of large cash deposits and unusual transaction patterns.

- Enhanced due diligence for high-risk accounts and Politically Exposed Persons (PEPs).

2.3 FATF Recommendations

The Financial Action Task Force (FATF) emphasizes a risk-based approach for detecting and preventing money laundering. FATF's guidelines highlight the importance of transaction monitoring, sanctions screening, and the use of technology to combat financial crimes.

The FATF Recommendations set out the essential measures that countries should have in place to:

- Identify the risks, and develop policies and domestic coordination
- Pursue detection of money laundering, terrorist financing and the financing of proliferation
- Apply preventive measures for the financial sector and other designated sectors
- Establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures
- Enhance the transparency and availability of beneficial ownership information of legal persons and arrangements
- Facilitate international cooperation

2.4 FIU-IND Guidelines

FIU-IND operates under the directives of the Prevention of Money Laundering Act (PMLA) of 2002 and aligns with international standards set by bodies like the Financial Action Task Force (FATF). FIU-IND provides detailed instructions on reporting suspicious transactions, including thresholds and timelines. The guidelines also encourage the use of advanced analytics for transaction monitoring and the adoption of mechanisms to prevent "tipping-off."

2.5 Indian Cybercrime Coordination Centre (I4C) Guidelines

The I4C under the Ministry of Home Affairs has issued specific advisories to banks and financial institutions on combating cyber-enabled financial crimes, including money mule activities. Key recommendations include:

- Using cybersecurity tools to detect unauthorized transactions.
- Monitoring accounts linked to known fraud cases.
- Collaborating with law enforcement to trace digital footprints.
- Regular awareness campaigns for customers to recognize phishing and mule recruitment tactics.

2.6 International Standards

Global bodies such as the United Nations and the European Union mandate cross-border collaboration and information sharing to address money mule activities effectively. They also encourage financial institutions to adopt robust sanctions screening and advanced analytics tools to monitor cross-border transactions.

---

3. Current Mechanisms to Tackle Money Mule Accounts

Banks and financial institutions currently employ a variety of tools and processes to identify and prevent the misuse of accounts as money mules. Key mechanisms include:

3.1 Know Your Customer (KYC) and Customer Due Diligence (CDD)

These are fundamental tools for verifying the identity and financial profile of account holders. During on-boarding and periodically, banks assess:

- The customer's source of income.
- Their geographic location.
- Relationships with other entities

3.2 Transaction Monitoring Systems (TMS)

Banks usually deploy rule-based systems to monitor transactions and flag suspicious patterns, such as:

- Large (Volume & Value) transactions by previously inactive accounts.
- Structuring, where a large amount is divided into smaller transactions to evade detection.
- High velocity transactions where the money is credited to account and debited in a short span of time
- Frequent international transfers or transactions involving high-risk jurisdictions.

3.3 Suspicious Transaction Reporting (STR)

Under regulatory requirements, banks report any unusual or suspicious activities to the Financial Intelligence Unit (FIU) for investigation when they detect or suspect that a transaction may be linked to illegal activities, such as money laundering, cybercrime or terrorist financing.

3.4 Sanctions Screening

Sanctions screening is the process of cross-referencing individuals, businesses, and transactions against blacklists of sanctioned parties. These lists, maintained by governments and international bodies such as Financial Action Task Force (FATF) and

United Nations Security Council, include those subjects to financial restrictions due to their involvement in illegal activities.

3.5 Cross-border Transaction Alerts

Transaction monitoring systems monitor frequent international transfers, especially those involving countries with weak AML frameworks. Banks usually carry out IP based transaction monitoring system and identification of unusual pattern of transactions both for domestic and from overseas jurisdictions. Further, regulators and law enforcement agencies provide inputs on cybercrimes being perpetrated from specific locations outside India, particularly from specific geographic hotspots.

3.6 Placing debit freeze / Hold on account

As per instructions of Cyberpolice on receipt of a complaint on the MHA Cybercrime.gov.in, Banks apply debit freeze on the reported fraud amounts. Few state (Gujarat, Himachal Pradesh) police authorities are also suggesting applying a complete freeze on debits from account up to layer 3.

4. Challenges in Current Mechanisms

Despite these mechanisms, significant challenges hinder their effectiveness due to various reason like:

- Regulatory variations
- Data quality and availability
- Evolving criminal threat
- Changes in the regulatory landscape
- Data and technology limitations
- High false positives

4.1 High False Positives

Rule-based systems generate numerous alerts, many of which are false positives. These overwhelm compliance teams and lead to resource inefficiencies. This occurs due to the rigid threshold values, over simplified approach to designing of rule engines and dependency on qualitative inputs to design the detection systems.

4.2 Latency in Detection

Most existing systems are not equipped for real-time monitoring. This could be due to various reason like technical limitations, lack of urgency for enabling real time core banking facilities for monitoring purpose. Delays in identifying suspicious activities allow criminals to move funds before action can be taken.

4.3 Limited Data Integration

Banks often face challenges to integrate external data, such as employment records, digital footprint or social media information, which could enhance the accuracy of risk assessments.

4.4 Adaptation by Criminals

Criminal networks constantly evolve their methods, outpacing the capabilities of static rule-based systems. Due to complex process of banking, it gets easier for the criminals to disguise the illicit activity as licit. Banks usually struggle to incorporate the changes at a faster pace to capture these trends of fraud and money laundering.

4.5 Resource Constraints

Smaller banks often lack the resources to invest in advanced monitoring systems or specialized personnel. Also, over reliance on the external service providers delays the process of continuous improvements in the monitoring systems due to time and cost components.

---

5. Proposed Mechanism Using Data Driven Detection Systems

A data driven detection system enables a computer program to learn continuously from data rather than through explicit programming. These programs work by taking historical or incremental data, finding patterns in it, that might be too complex for an analyst to intuitively see, then applying the findings to new data. When this learning capability is coupled with adequate computing power, such systems can be developed that can detect complex patterns and make decisions in an automated way. To strike a balance between regulatory compliance, fraud risk management, and customer expectations, banks and FinTech's need to implement such sophisticated monitoring solutions. To achieve this, there should be processes, systems and tools with automated workflows that:

- Connect to more alternative data sources
- Provide more high-quality, real-time data that accurately verifies transaction legitimacy
- Breakdown data silos that impede efficient integration, sharing, and data analysis
- Build holistic customer, account and transaction profiles for accurate portfolio monitoring

When the relevant and specific data is equally shared across teams, departments and ultimately banks, it can be used to enhance overall risk visibility and quick identification of suspicious behaviour. As a result, banking industry as a unified entity can stop fraud and money laundering activity. Efficiency can be brought in by collaborating with one another and optimizing inter-organization strategies and processes in tandem; rather than continuing to work within the confines of own data silos.

The proposed mechanism introduces data driven systems backed by AI and ML to enhance detection capabilities, reduce false positives, and improve response time and overall efficiency. The key components of the mechanism include:

5.1 Data Enrichment

- **Overview:** Data enrichment is about enhancing the information associated with financial transactions. It goes beyond the basic transaction data and includes additional details about the parties involved. Enriched data could provide additional information, such as the location of the customer at the time of the transaction, location specific geo-political risk, transaction device details, recent transaction history and even behavioural patterns associated with the customer. By analysing this enriched data, it becomes easier to detect deviations from normal behaviour and to flag suspicious transactions for further analysis.
- **Implementation:** Banks should initiate and strategize the process of data enrichment by exploring various tools and setting up clear vision for acquiring and deploying the same. This can help to collect, process, and analyse data from a variety of sources, such as public records, social media and negative registry to detect and prevent fraudulent activity more effectively.

5.2 Behavioural Analytics

- **Overview:** This method analyses individual customer behaviour in comparison to their historical patterns and peer group norms. It aims to detect unusual deviations that may signal activities related to digital payment fraud or money laundering. Behavioural analytics focuses on individual level activities, enabling the detection of subtle anomalies that might be overlooked by other methods which focuses on entire portfolio or product level.
- **Implementation:** A multi-phase monitoring system is ideal for behaviour analytics, where the various phases capture the behavioural aspect of each stage of customer life cycle. An effective behaviour analytics model will be able to distinguish between suspicious activity and normal activity by comparing the customer with each peer group and past transaction patterns. As the definition of suspicious and normal could change based on the context, a dynamic analytical model should be preferred for implementation.

5.3 Anomaly Detection Models

- **Overview:** Anomaly detection is the identification of events or transactions that deviate from what is usual, standard or expected, making them inconsistent with the rest of the observations. The AI/ML based anomaly detection models can analyse the customer portfolio and each of its transaction by focusing on customer profile, account type, transaction amount, possible motive, frequency, velocity and consistency with the previous activity and the geographic location to precisely identify anomalous activities.
- **Implementation:** A common but effective approach to building and implementing anomaly detection systems is to combine the Unsupervised and Supervised machine learning techniques. With unsupervised machine learning, the algorithm learns from sample data that has not been labelled, classified or categorized. The algorithm is on its own to find structure or hidden patterns in

the data. This also helps to discover new patterns which was earlier unknown to the analysts. With supervised machine learning, the model is presented with historical inputs and their associated outputs, and the goal is to uncover the patterns that maps those inputs to outputs. By doing so, the model learns how to better predict the outcome when it is applied to new data.

5.4 Real-time Monitoring

- **Overview:** Real-time transaction monitoring analyses transactions as they happen, allowing for immediate detection and response to suspicious activities. It enables quick intervention by means of freezing the account or declining the transaction, hence reducing opportunities for criminals to launder money, enhancing customer protection, and maintaining the integrity of the financial system.
- **Implementation:** This strategy involves continuously analysing data, transactions, or user behaviours in real time. It is often used along with other measures like device fingerprinting, identity graphing, and supervised machine learning. Real-time monitoring should be integrated with machine learning models which continuously review transactions to immediately detect and respond to potential suspicious behaviour as it happens. Automated action can be taken by integrating the alerts to core banking systems and digital payment platforms.

5.5 Network Analysis

- **Overview:** Network analysis can use network data, such as financial transactions, customer profiles, or suspicious activity reports, to construct and analyse the money laundering networks, such as the placement, layering, or integration stages, the source, destination, or intermediary money mules, or the amount, frequency, or complexity of transactions. At its core, network analysis is the study of how entities relate to one another.
- **Implementation:** Banks should leverage the graph theory, which forms the backbone of most network analysis techniques. In the AML context, graph-based techniques can be employed by banks to:
    - Identify key players in a transaction network
    - Detect clusters within networks, revealing groups of accounts or entities that frequently transact with one another
    - Measure network density, which can give insights into the level of interconnectivity within the network
    - Study sequence patterns to understand the order in which transactions occur, revealing laundering steps or cycles
    - Separate transaction types into distinct layers (e.g., Online transfers, Cash withdrawals, Crypto exchanges etc.)

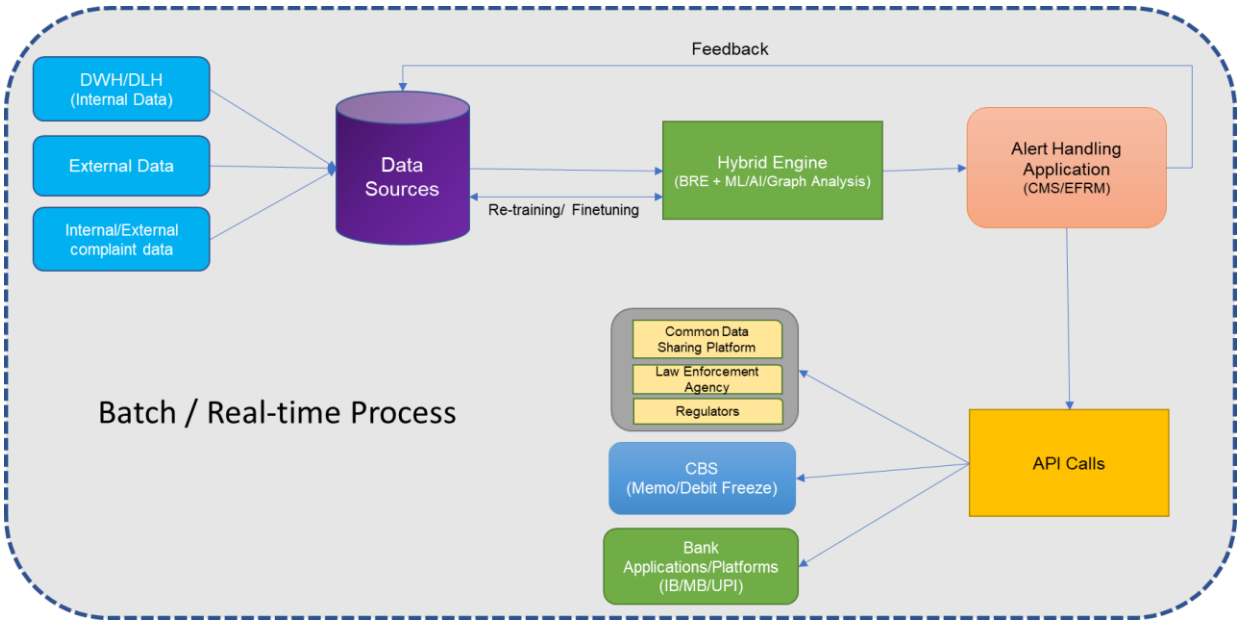
5.6 Explainability of Models

- **Overview:** Model explainability refers to the ability to understand and explain how an artificial intelligence or machine learning model arrives at its decisions,

which makes the complex algorithms more transparent and interpretable. As the components of financial transactions are highly sensitive, it is not enough for an AI/ML model to simply flag a transaction as suspicious. It's crucial to understand why the model made that determination.

- **Implementation:** Achieving explainability in complex AI/ML models can be challenging. However, suitable techniques and tools should be adopted or developed by the banks for:
    - Regulatory Compliance: Explainable AI/ML systems help banks demonstrate to regulators and law enforcement agencies that their systems are fair, unbiased, and effective.
    - Enhanced Trust and Accountability: When analysts understand why a model flags a transaction, they can better assess the risk and make informed decisions. This is significant to increase the trust in the system and ensures accountability.
    - Improved Accuracy and Efficiency: Explainability helps identify potential biases or weaknesses in the model, leading to improvements in accuracy and a reduction in false positives.
    - Effective Communication: Explainable AI/ML systems facilitate communication between technical experts, business stakeholders, regulators and law enforcement agencies.

Indicative Workflow



6. Pre-onboarding Checks:

This section provides guidance on effective screening of the cases, as part of the Pre-onboarding as a due-diligence perspectives. These checks can help in mitigating the risk of money mule entering the financial ecosystem.

6.1 Pre-onboarding – KYC & Due Diligence checks

- Due Diligence & KYC document checks by Sourcing Staff. KYC to be done in true spirit – Verify and validate customer profile and not just collect OVD documents.
- Banks should have comprehensive procedure manuals on customer pre/post onboarding and reviewing KYC documents, ensuring that all staff members have easy access to them. This is critical for maintaining consistency, compliance, and efficiency in operations.
- Information captured on CKYCR through KYC identifier, where consent of the customer is obtained.
- Risk based onboarding – Higher risk accounts to be approved by senior officials
- GST fetch in case of current accounts & Seek income proof in case of abnormal turnover quoted by customers with lower vintage
- Customers applying to open current accounts with a new/recent GST registration and a new rental/tenancy agreement, banks should implement additional verification measures such as Surprise Visit to Business Address, Neighbourhood Inquiries, Cross-verification with documents. If any red flags are found, same may be escalated internally to AML team for their review and further escalation to FIU, India if deemed necessary. And may also add such customers name in internal suspect registry to avert such attempts at other branches of the bank.
- For Sole Proprietorship cases, conduct thorough due diligence with respect to business profile, activity, promoter background, understanding of business they are into, expected turnover etc.
- Banks to have processes in place to assessing the new customers business legitimacy, financial standing, and readiness for launch. Check whether the businesses are using third-party contracts (surrogate contracts). And also verify whether the business has the necessary resources, permits, and structures to function effectively.

6.2 Digital onboarding checks suggested for effective screening:

a. Improved PAN checks Via Protean (Integration of NSDL new API and PAN+API

b. Validate OVD (Officially Valid Documents) such as Aadhaar from UIDAI records through E-KYC authentication

c. Name match between PAN and Proof of Identity.

d. Restricting the use of a unique email ID and mobile number for onboarding through digital channels. This action will prevent multiple registrations with the same email or phone number, reducing duplicate

or fake accounts. Also implement enhanced authentication by requiring OTP validation for both email and mobile.

e. Flagging provided if the Mobile number entered in the onboarding journey is not linked with Aadhaar. It should not be mandatory conditions that only Aadhar Link Mobile number is allowed.

f. Customers Mobile Number & Email id verification via OTP authentication. Currently, the Department of Telecommunications (DoT) provides a list of MNRL (Mobile Number Revocation List) numbers. Any suspicious mobile number flagged should be denied onboarding. API integration with the DoT / TSPs (Telecom Service Providers) can be used in the digital onboarding on account opening. The name, date of birth, and email address can be verified in real time from the Mobile service provider DoT. This information is available on a consent basis. The address can be another factor.

g. Live photo capturing utility, The Centre for Development of Telematics (CDOT) has developed the Advanced Security Telecom Research (ASTR) model, which can be leveraged for enhanced fraud prevention. ASTR maintains a database of approximately 1.4 billion mobile numbers, linked to images of the individuals to whom the SIM cards were issued. Critically, this database also includes images of known fraudsters who have utilized multiple SIM cards under different names but with the same identifying image. This allows for the detection of individuals attempting to use fraudulent identities.
    - ✓ API integration with the ASTR system is possible, enabling real-time verification during the onboarding process. Beyond the image and mobile number association, ASTR may also contain additional information that can be valuable for fraud detection. This could include:
    - ✓ **KYC Details:** Information provided during SIM card registration, such as address, identity document details (e.g., Aadhaar, Voter ID), and potentially biometric data.
    - ✓ **Linkages:** ASTR might provide information about connections between different mobile numbers, helping to uncover networks of fraudsters.
    - ✓ **Complaint History:** Records of complaints filed against specific numbers or individuals could indicate a history of fraudulent activity.
    - ✓ By integrating with the ASTR system and utilizing the full range of available data, organizations can significantly improve their ability to identify and prevent fraudulent activity during customer onboarding on consent based.

h. Dedupe checks in the system. All Core Solutions have this functionality and if not such functionality must be developed by all banks.

i. Negative database screening check. There are multiple sources of negative registry 1. Suspected Registry available in I4C portal, DOT MNRL, and RBI CFR , The Integration with all these must be ensured

j. Banks should establish their own register of suspect or designated persons and entities, integrating it with the customer onboarding process to prevent the on-boarding of identified individuals or entities.

k. In case of On-boarding journey through V-CIP mode, negative PIN Code restriction is checked.

l. Geo tagging data captured while onboarding. Geo Tagging of all BCs is must, and V-KYC and online account opening must have such monitoring and intelligence

m. Additional Due Diligence on the occupation, turnover and income:

- Banks should implement processes and procedures to verity a customer's occupation and expected turnover, ensuring alignment with the income reported by the customer. (ex. The customer's declared income does not align with their lifestyle).
- Farmer/landless labour quoting income of 1 lakh per month.
- Housewife quoting the income of above 5 lakhs but no ITR filed. The maximum threshold should not be more than Rs 10 Lakhs where ITR is not available. The bank should have the option to freeze accounts or disable digital channels whenever the quarterly threshold is breached (excluding transactions from our accounts). Banks should have the option to exclude some of the transactions from threshold calculations.

6.3 Validation of OVDs:

i. Aadhaar is being verified from the UIDAI database. Other documents can be verified from the below mentioned portals:

S.No	Identity document/Number	Source for verification
1	Election ID card	VOTERS' SERVICES PORTAL (eci.gov.in) (https://electoralsearch.eci.gov.in)
2	Passport number	Passportindia.gov.in<<Track application status
3	Driving license	https://parivahan.gov.in/ or Official websites of Transport authorities of respective states as some states are not integrated with Parivahan)
4	GST NUMBER	https://services.gst.gov.in/services/searchtp (APIs available)

5	CIN	https://www.mca.gov.in/content/mca/global/en/mca/fo-llp-services/findCinFinalSingleCom.html
6	NPO UNIQUE ID	https://ngodarpan.gov.in/index.php/search/
7	DIN	https://esanchar.cbic.gov.in/DIN/DINSearch
8	IMPORT EXPORT CODE	https://www.dgft.gov.in/CP/?opt=view-any-ice
9	LLP IN	https://www.mca.gov.in/content/mca/global/en/mca/fo-llp-services/find-llpin.html
10	UDYAM REGISTRATION CERTIFICATE	https://udyamregistration.gov.in/udyam_verify.aspx
11	IT RETURNS	https://incometaxindiaefiling.gov.in/

** NPS details, PF details, Passport details ,Driving License Details can be fetched thru API Integration as there are many Technical Service Providers , But these are all Consent based .

All the portals mentioned above can be accessed through intranet. However, direct APIs are not available for the Banks to integrate with them directly and to validate them from the source.

ii. Though Election id card is an officially valid document, it can be validated from source only if it is issued recently or if the voter has been updated in the lists recently. In absence of validation of the same, it is not possible to identify original and fake Voter ID card.

There is no challenge in getting information from Mobile Service Providers (MSPs) on a real-time basis with the help of Technical Service Providers (TSPs), or banks can create their own API to fetch data from MSPs with customer consent. Data can be pulled from MSPs in real-time. The challenge lies in:

1. How to manage mobile numbers if they are allowed or have been allowed in multiple customer IDs.
2. How to educate account holders not to become mules unknowingly, knowingly, or complicity.

At the time of account opening, personal information, including name, mobile number, email ID, and address, can be fetched from MSPs in real-time with the customer's consent. If the address and email fetched from MSPs do not match the details available in Officially Valid Documents (OVD), such a mismatch should not be the sole criterion for rejecting the account opening, particularly the address fetched from MSPs. The challenge is that one mobile number is allowed for different customers, particularly family accounts. There needs to be a defined policy applicable across the bank on

how many customer IDs one mobile number can be allowed and, if allowed, what additional undertakings or OVDs need to be taken.

6.4. Controls pertaining to location/distance:

- Account opening is allowed only if the distance between the geolocation from where account application is initiated is within 50 km distance from the location where Video KYC for the same application is attempted and 25 km for onboarding through BC channel. (Redraft) Extra due diligence needed if it is beyond their limit.
- Practice of hotspot check i.e. blacklisting of fraudulent latitude/longitude reported and velocity check by restricting number of accounts that can be opened from a particular location in same month while onboarding customer through digital channel.
- To ensure/verify that the field visit officer is visiting the actual place of verification, Geo-tagging process has been implemented wherein Pin code of Geo-coordinate location of Sales executive is cross checked with customer's communication address captured in the system (based on OVD/declaration based on Aadhaar biometric authentication).
- Leveraging tech to identify lat-long of customers, liveliness check, forgery check, identify identity theft, fetch customer details through document issuing portals like GST directly

6.5 Initial funding related controls:

- While onboarding customers through digital mode, Bank to ensures that the initial funding is carried out through customer's own KYC compliant account and not from any third party.
- Initial funding in cash is being restricted in onboarding through BC channel.

6.6 Due diligence measures using Tech enablers:

- Validation checks to ensure the IP address is not spoofed is captured on WorkApps (Video KYC platform).
- Customers cannot do video KYC from location belonging to a list of negative hot spot locations
- To restrict number of accounts that can be opened from a particular location in the same month.
- Revamp of Video KYC script and standardised across all products with addition of extra blocker questions and product relevant profiler questions in VKYC script implemented.
- Fraud Model Check- Basis the application parameters shared by customer and collected from customer's device, the model runs real time to assess the

propensity of the customer to be fraudulent, during end-to-end digital onboarding.

- Statistical Models for various customer segments at the onboarding stage. Enhancing Core Banking System to generate transaction alert and placing transaction restrictions on near real time basis.
- Automated data fetching from regulatory sites
- Granting online transaction limits basis customer risk profiling

7. Post-onboarding checks / monitoring:

Financial institutions must establish a thorough post-onboarding monitoring framework to maintain continuous compliance of customers following the completion of the onboarding process. This framework should encompass regular monitoring, detailed analysis of customer activities, and periodic reviews to quickly detect and resolve any compliance issues.

The key activities include:

- Monitor the return of welcome kits and other correspondence to ensure the accuracy of the customer's provided address. Any returned mail should be reviewed promptly to identify potential discrepancies, verify the correctness of the address, and take necessary follow-up actions to update or validate customer details as needed.

  Proposed Procedure:
  - Bank correspondence/deliverables undelivered due to the reasons like address not found/client not residing at the address, shall be considered for enhanced due diligence especially considering that V-CIP sourced clients are allowed to declare their current address which is not getting verified through any documents.
  - These customer relationships should be closely monitored, and temporary restrictions should be placed on digital channel access and bulk transfer facilities till the time client do not produce proper address and successful delivery.

- **Monitor Initial Deposits:**

  - Closely monitor accounts that receive initial deposits from the same UPI IDs or PhonePe IDs, as this may indicate that the accounts are being opened on behalf of others. Such patterns raise the likelihood of money mule activities, where accounts are used to facilitate unauthorized or fraudulent transactions. Enhanced scrutiny and due diligence should be applied to identify and mitigate potential risks associated with such accounts.
  - Monitor requests for address and mobile number changes that occur immediately after customer onboarding, as frequent or sudden changes may indicate fraudulent activity. Further, restrict the ability to change mobile

numbers through ATMs or online banking services for newly onboarded customers to prevent unauthorized modifications and enhance security. Any such attempts online/requests should undergo further verification to ensure authenticity.

- Track requests for any updates to customer profiles, including changes to mobile numbers, email addresses, and correspondence addresses. These alterations should be closely monitored to identify any suspicious or unusual activity.

Proposed Procedure:

- Instances of multiple times updates in the client contact details like email no, address etc. during initial period from account opening say 60 Days, shall be considered for enhanced due diligence.
- Any modification in Mobile number for accounts are not allowed till the completion of initial 60 days from a/c opening date through Mobile Banking/Internet Banking /ATM.

- **Monitoring Unusual Activations**:
  Track mobile and online banking transactions from location distant from the customer's registered/correspondence address. Utilize tools to monitor overseas IP addresses to identify such transactions including activations from overseas locations.

- **Closely monitor the rapid registration of new beneficiaries**
  Track the rapid registration of new beneficiaries, which could be unusual or suspicious activity.

- **Registration of suspected entities as beneficiaries**:
  - Track the attempts to register suspected or high-risk entities as beneficiaries. This includes flagging and reviewing such registrations to prevent fraudulent activities.

- **Debit Card Activation Monitoring**:
  - Track debit card activations at ATMs located far from the customer's residential address or fraudulent activities.

- **Monitoring Numerous Login Attempts Shortly After Account Opening:**
  - Monitor numerous attempts to access banking services shortly after an account is opened.
- **Same Customer Logging in from Multiple Locations on the Same Day:**
  - Watch for cases where the same customer logs in from multiple geographic locations on the same day, as this may suggest account compromise. Banks eFRM Solution should be capable of preventing such efforts.

- **Flagging Customers with Unusual Email Addresses:**
  - Identify and monitor customers with email addresses that appear unusual or suspicious, as this can be an indicator of fraudulent activity or attempts to mask identity. Define it such as xyz@gmail.com.

- **Detecting Same IP Address Used by Different Customers on the Same Day:**
  - Monitor for instances where the same IP address is used by different customers on the same day. This could indicate potentially fraudulent activity or coordinated actions by multiple accounts.

- **Monitoring high volume, round figure, near-round figures, or small amount transactions:**
  - A high volume of transactions in an account involving round figures, near-round figures, or small amounts- typically ranging from Rs.10 to Rs.5000- without sufficient justification based on the customer's profile should be closely monitored. Such transaction patterns may indicate potential suspicious activity, including structuring or layering of funds to evade detection. Enhanced scrutiny should be applied to identify any anomalies, verify the legitimacy of transactions.

- **Suspect Registry and de-dupe against banks database**:
  - Banks to onboard to the Suspect Registry of I4C, Ministry of Home Affairs for Preventing Cyber-enabled Frauds in line with RBI Advisory dated 31 December 2024, which can be used for de-duping against bank's clients for preventing cyber-enabled frauds. Banks to also need to provide inputs in the Suspect Registry for any potential cases of money mule identified.

- **Other Special Focus Areas for consideration**
  - To give highest importance to information sharing between banks
  - Filing of FIRs against money mule account holders may be considered with legal consent
  - Implementing contact point verification in hotspot areas
  - Banks to participate in the MuleHunter.ai of RBIH.
  - Special focus on any resourcing of clients related issue e.g. set of clients sourced through specific branch or RM which might be facilitating group of potential money mule accounts.
  - Enhanced Due Diligence of current accounts wherein there are huge volume of transactions, inconsistent with the declared turnover and business profile.
  - Customers with part-time job, housewife, self-employed profile and receiving high volume of transactions such as high salary payments, commissions, etc in short span of time.
  - Scenarios where new credit facilities e.g. loans are applied based on existing relationship then certain set of documents like income proof etc.

shall be revisited/reverified to eradicate scenarios where there might be cases where fabricated income documents could have provided while availing initial product offering e.g. credit card.
- Maintain strong customer relationship and customer interactions to identify potential threats.

8. Portfolio Monitoring:

Key Components of a Money Mule Portfolio Monitoring Framework and effective portfolio monitoring requires continuous access to transactional data, customer behaviour, and historical records of the customer. This will help through behavioural analysis and anomaly detection to frame a predictive modelling tool through Machine learning algorithms to identify potential red flags and detect deviations from normal patterns.

8.1 Data Collection and Integration

Based on various data, behavioural pattern, transactions pattern and other data regarding the profile of customer including KYC details, geographical location, transaction frequency, etc., a number of RFIs (red flag indicators) listed out below which are common characteristics of money mule / potential money mule accounts.

- Customer with low-income group(s): Accounts having declared income of less than Rs.0.50 lakh and Between 0.50 lakh and Rs.1.00 lakh.
- Profile/Occupation: Customer with declared profiles as Agriculture labourer, Unemployed, Students, Graduate, Undergraduate, Service in Private Company and Housewife etc. with high turnover.
- Account Type: Special monitoring of the accounts opened with minimum KYC requirements.
- Demographic Hotspots: Customer belongs to demographic hotspots/locations where the money mule accounts are opened and operated to perpetrate cyber-crimes e.g. Bharatpur, Mathura, Nuh, Deoghar, Gurgaon and Alwar etc.
- Customers aged between 18 and 25 years who exhibit a high volume of financial transactions in their accounts that appear inconsistent with their stated occupation and declared income.
- Mode of transactions: The mode of transactions be high number of online transfers of small amounts through UPI/IMPS/Mobile transfers/digital payment gateways in short period immediate after opening of the account in many to one & one to many forms.
- Cash transactions: High number of small amount cash transactions – cash deposits over the counter at home / non-home branches, card deposits /card less cash deposits through cash deposit machines at remote locations. Also, withdrawal of cash through ATM at different locations away from the home branch.

- Multiple Accounts: Customers maintaining multiple accounts with different banks having similar VPA for all accounts, multiple VPAs for single account and all the accounts linked to one mobile number etc.
- Frequent Updating of mobile number: Frequent change of mobile numbers observed – some mobile number(s) been rotated between group members. New Mobile updated, Mobile number already linked to other customer account etc.
- Activation of dormant account: Accounts lying dormant for many years been activated and immediate high number of digital transactions carried out with in a very short span of period.
- CBDC (Central Bank Digital Rupee) Wallet loading: Customer's CBDC Wallet loaded by transferring funds from different banks by many different parties followed by redemption of the funds and transferring to many other parties/withdrawing cash at different locations.
- Multiple, rapid transfers to and from different accounts.
- Transactions involving high-risk geographies.
- Abnormal transaction volumes or frequencies compared to historical behaviour.
- Unusual merchant activity or cross-border transactions.
- Ensure that alerts are generated and examined in case of abnormally frequent and large transactions in domestic bank accounts being carried out from locations including from overseas jurisdictions, not matching with the usual location / economic / financial profile of the customer.
    - Put in place an IP based transaction monitoring system and identify unusual pattern of transactions both for domestic and from overseas jurisdictions. Further, in view of the recent inputs on cybercrimes being perpetrated from locations in Southeast Asia, particularly from Cambodia, Myanmar and Laos PDR and any specific countries based on the latest updates, special attention may be provided to Indian bank accounts being operated from such jurisdictions. The necessary inputs in this regard may also be obtained from I4C, MHA, GoI on a regular basis. The banks may also put in place restriction on usage of transaction from overseas IPs, based on the customer profile;
    - Monitor cash withdrawals made through overseas ATMs and at ATMs outside the State where the customer resides or at locations which are hotspots and examine the need for transaction restrictions on use of Indian Debit Cards abroad, especially from Dubai, Kazakhstan and Thailand and any specific countries based on the latest updates.
    - Monitor cash withdrawals through cheques made from domestic branches of banks especially in hotspot regions. Necessary inputs in this regard may be obtained from I4C, MHA;
    - Monitor loading of prepaid wallets issued by foreign entities, using domestic debit / credit cards / bank accounts

8.2 Baseline and Risk Profiling

Establish a normal behavior profile for customers to identify deviations:

- Segmentation: Group customers based on risk categories (e.g., age group, income, geography, occupation etc.).
- Baseline Profiles: Use historical data to set benchmarks for normal activity.
- Risk Scoring: Assign scores based on attributes like high-risk jurisdictions, unusual transaction volumes, or inconsistent income patterns.
- Banks should establish comprehensive procedure manuals to systematically identify and analyze unique customer behavior based on various common characteristics. Further, they should implement a dynamic risk-scoring matrix that evaluates each characteristic of a customer, aggregates the overall customer risk score, and assigns an appropriate risk category.
- To enhance KYC/AML risk management, banks should define clear thresholds for each risk category, classifying customers as Low, Medium/Moderate, or High risk based on their aggregated scores. Furthermore, specific thresholds should be introduced to trigger enhanced monitoring for accounts that exhibit unusual or high-risk activities, ensuring proactive identification and mitigation of potential financial risks.

8.3 Monitoring and Detection:

Develop automated and manual processes to monitor and flag suspicious accounts:

Rule-Based Triggers:

- Large or rapid fund inflows followed by immediate outflows.
- Uncharacteristic activity for the customer’s profile.
- Frequent small transactions to multiple recipients (smurfing).

Machine Learning Models:

- Anomaly detection models to flag unusual patterns.
- Predictive analytics to identify potential mule accounts.

8.4 Investigation and Reporting:

Verify flagged accounts to determine if they are legitimate:

- Contextual Review: Analyse flagged transactions in the context of the customer's historical data.
- Enhanced Due Diligence (EDD): Reach out to the customer for additional documentation if needed.
- Internal Reporting: Escalate cases to the AML/CFT team for detailed review.
- External Reporting: File Suspicious Transaction Reports (STRs) with the relevant authorities (FIU India) and providing data to LEAs like I4C etc.

9. Transaction Monitoring, Trigger Basis Alternate Data Feed (NPCI / NCRP):

Traditional transaction monitoring systems rely on limited internal transaction data, which may not always provide a full picture of suspicious activity. By utilizing alternate data feeds from NPCI and NCRP, banks can gather comprehensive transactional data, improving their ability to detect and mitigate money mule risks.

NPCI: As the backbone of India's payment systems, NPCI provides transactional data on payments made via IMPS, UPI, AEPS, and other payment networks. This data is essential for tracking real-time financial flows and identifying patterns that may indicate money mule activity.

NCRP: The National Cyber Crime Reporting Portal serves as a centralized platform for citizens in India to report various types of cybercrimes. It aims to streamline the reporting of cybercrimes, enhance coordination between law enforcement agencies, provide timely interventions, and promote cybersecurity awareness across India.

Covering following key areas:

- **Data Integration:** Incorporating NPCI and NCRP data into the existing transaction monitoring system.
- **Alert Generation:** Establishing triggers based on predefined parameters, such as rapid fund movement, unusual patterns, and high-risk geographies, use of AI/ML Technology for alert generation.
- **Data Sharing Protocols:** Implementing standard operating procedures (SOPs) for real-time data sharing between banks.
- **Fraud Detection:** Leveraging machine learning and analytics to identify potential mule accounts and transactions.
- **Regulatory Compliance:** Ensuring compliance with financial regulations regarding fraud detection and data sharing.
- **Customer convenience:** Ensuring that genuine customer is not affected in the process of controlling menace of money mules.

Process Flow:

- **Data Collection and Integration:**

The transaction monitoring system should receive and integrate real-time transaction data from NPCI (e.g., UPI, IMPS) and Cyber Fraud related data from NCRP I4C and based on this data the system should continuously update financial profiles and transaction histories, providing a holistic view of customer behaviour.

- **Other Scenarios**
  - Strengthen policies, procedures, systems, and controls to prevent cyber- enabled frauds and the use of money mule accounts.
  - Exercise care and due diligence in recruitment and deployment of employees for customer on boarding and due diligence processes
  - Fix staff accountability for non-adherence to KYC/AML/CFT regulations and misuse of accounts.
  - Restrict access to customer databases to authorized officials and monitor data shared with third-party vendors or outsourced agencies.
  - Ensure prompt action/ Responses on requests from Law Enforcement Agencies (LEAs) and Indian Cyber Crime

Coordination Centre (I4C), MHA.

- Adhere to directions on the introduction of new technologies and assess ML/TF risks before launching new products/services
- Ensure synergy and coordination between anti-fraud and AML/CFT controls.
- Deal sternly with money mule accounts without any delay and ensure compliance with KYC/AML/CFT regulations.
- Ensure strict adherence to customer due diligence requirements during opening of accounts and monitoring of newly opened accounts, in order to restrict mule accounts and their operations
- Carry out a comprehensive analysis of the accounts being used/ identified as suspected money mule accounts and strengthen the risk monitoring rules based on the same
- Review various customer onboarding processes adopted by the bank and address the gaps / vulnerabilities being exploited by the fraudsters, particularly in accounts opened through non-face-to-face mode, V-CIP, Aadhaar OTP based e-KYC accounts, accounts opened from particular areas / locations where frauds/cybercrimes are more prevalent (hotspots) etc
- Ensure deployment and adoption of robust software for real-time transaction monitoring and use of AI / ML tools in detecting suspicious and fraudulent transaction patterns as well as use of network analytics in identifying mule networks. Setting up of a dedicated centralised unit at the bank-level may also be considered for a harmonised and time bound response in countering cyber-enabled frauds
- Fix a shorter Turn-Around -Time (TAT) for processing alerts pertaining to money mules cyber-enabled frauds and for reporting STRs, as may be required
- Have a robust mechanism for change of mobile number by customers, and also monitor such customers who frequently change their mobile numbers, through Enhanced Due Diligence
- Carry out Enhanced Due Diligence of current accounts wherein there are huge volume of transactions, inconsistent with the declared turnover and business profile, as in many cases, it has been observed that current accounts opened by Sole Proprietorship firms using Udyam Registration Certificate (MSME) are used to transfer / layer the proceeds of crime
- Subject accounts that are being repeatedly reported on the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) to Enhanced Due Diligence and take action as per PML Act,2002 and analyse such accounts on the reasons for opening and their repeated usage in channelling fraudulent proceeds. In this regard, any instruction received from Law Enforcement Agencies (LEAs) shall be adhered to as per the extant law
- Include the typologies on cyber-enabled frauds and use of money

mule accounts as part of the training curriculum in the bank, so as to sensitise the staff, particularly those who are required to deal with KYC / AML matters and Transaction Monitoring.

- **Final Action:**

Once the account is identified as suspected mule account / mule account action to be initiated against the account holder such as:

- Giving information back to LEAs
- Creating internal negative registry within the bank.
- STR Filling

10. Real time sharing of fraudulent transactions data between banks

- **Data Encryption and Security:**
  - All shared transaction data must be encrypted to protect sensitive information.
  - The data exchange platform must comply with relevant data protection and privacy laws.

- **Cross-Bank Data Sharing Platform:**
  - Banks will use a secure centralized platform to share fraudulent transaction data, ensuring that all parties involved have access to the most up-to-date information.
  - The platform will allow for the immediate dissemination of flagged transactions to other financial institutions.
  - The platform should take data from multiple dimensions like CFR, I4C, ECGC, TRAI etc. for the use of entire ecosystem.

- **Reporting and Escalation:**
  - In case of confirmed mule activity, the bank must immediately notify all relevant financial institutions within the network, ensuring the suspension or freezing of involved accounts.
  - Each institution must designate a nodal officer responsible for reviewing alerts and ensuring the timely sharing of information.

- **Regulatory Compliance:**
  - The SOPs will align with AML regulations, including mandatory reporting to regulatory authorities within prescribed timeframes (e.g., within 72 hours).

11. Expectations from Banks

Banks and other FIs play a critical role in the success of this framework. Specific expectations include:

11.1 Investment in Technology

- Adopt AI/ML-powered systems for transaction monitoring.
- Upgrade legacy systems to enable integration with advanced tools.

11.2 Staff Training

- Train compliance teams to understand AI/ML tools.
- Ensure staff can interpret AI-generated alerts.

11.3 Collaboration and Information Sharing

- Participate in industry forums to share insights and best practices.
- Collaborate with FIUs and other financial institutions to improve detection.

11.4 Adherence to Regulatory Standards

- Implement the risk-based approach outlined by FATF and FIU guidelines.
- Ensure timely reporting of suspicious transactions.

11.5 Periodic Audits and Assessments

- Conduct regular reviews of transaction monitoring systems to identify gaps.
- Adjust models based on evolving criminal methodologies.

12. Role of Law Enforcement Agencies

Law enforcement agencies are pivotal in dismantling money mule networks and prosecuting offenders. Their roles include:

12.1 Collaboration with Financial Institutions

- Work closely with banks and FIUs to investigate flagged transactions.
- Share intelligence on known mule accounts and criminal networks.

12.2 Use of Advanced Technology

- Employ forensic tools to trace the flow of illicit funds.
- Analyze data provided by banks and other financial institutions to identify patterns.

12.3 Training and Awareness

- Conduct workshops for banks on identifying and reporting money mule activities.
- Provide feedback on STRs to improve the quality of future reports.

12.4 Cross-border Cooperation

- Collaborate with international agencies to track and apprehend criminals operating across jurisdictions.

13. Expected Benefits

13.1 Enhanced Accuracy

AI/ML systems significantly reduce false positives, allowing compliance teams to focus on genuine threats.

13.2 Proactive Detection

Real-time monitoring prevents funds from being laundered before detection.

13.3 Resource Optimization

Automation reduces the need for manual reviews, saving time and costs.

13.4 Scalability

Advanced systems can handle increasing transaction volumes without degradation in performance.

13.5 Improved Regulatory Compliance

Enhanced capabilities ensure adherence to FATF recommendations and local AML laws.

14. Conclusion

The fight against money mule accounts demands a dynamic, technology-driven approach. By integrating AI and ML into transaction monitoring systems, banks can address existing gaps, anticipate criminal strategies, and protect the integrity of the financial ecosystem. A concerted effort involving investment in technology, staff training, and collaboration among stakeholders will ensure a more secure financial landscape.

This framework represents a blueprint for curbing money mule activities. Implementing these measures will require dedication and cooperation from financial institutions, regulators, law enforcement agencies and technology providers. Together, we can safeguard the financial system against evolving threats and the menace of money mule accounts.

15.Abbreviations used

AEPS	Aadhaar Enabled Payment System
AI	Artificial Intelligence
AML	Anti-Money Laundering

AML / CFT	Anti-Money Laundering and Combating the Financing of Terrorism
CBDC	Central Bank Digital Rupee
CDD	Customer Due Diligence
CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
DWH / DLH	Data Warehouse / Data Lakehouse
ECGC	Export Credit Guarantee Corporation
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institutions
FIU-IND	Financial Intelligence Unit of India
GoI	Government of India
I4C	Indian Cybercrime Coordination Centre
IMPS	Immediate Payment Service
KYC	Know Your Customer
LEA	Law Enforcement Agencies
MHA	Ministry of Home Affairs
ML	Machine Learning
MSME	Ministry of Micro, Small and Medium Enterprises
NCRP	National Cybercrime Reporting Portal
NPCI	National Payments Corporation of India
PDR	People's Democratic Republic
PEPs	Politically Exposed Persons
PMLA	Prevention of Money Laundering Act
RBI	Reserve Bank of India
RFI	Red Flag Indicators
RM	Relationship Manager
SOP	Standard Operating Procedure
STR	Suspicious Transaction Reporting
TAT	Turn-Around -Time
TMS	Transaction Monitoring Systems

TRAI	Telecom Regulatory Authority of India
UPI	Unified Payments Interface
VPA	Virtual Payment Address
V-CIP	Video Based Customer Identification Process

16. Suggestions:

Reserve Bank of India:

- The instructions may be issued that, Voter ID card can be accepted as Officially valid document provided it can be validated from election commission of India website (https://electoralsearch.eci.gov.in).
- Some FIN TECHs are providing APIs for verification of customer data and history based on mobile numbers. They are obtaining data from Telcos and providing the details like history of mobile, owner particulars, social profile based on data available on various social media platforms, credit history and availability of the same mobile number in Suspect registry of I4C etc. Guidelines may be provided in utilizing the services of these fintechs as much information can be sought based on the mobile numbers and this also ensures the mobile number of the account holder only is fed in the system. This will also ensure that fraudsters does not take the control of the Money mule accounts by updating their mobile numbers.
- We have around 11 Crore income taxpayers, who are registered users in income tax portal. Number of PAN card holders are much higher than the number. However, there is no specific limit on transactions to be allowed though account is opened with form 60. As annual income is one of the major parameter for generating RED flag indicators, guidance may please be provided on limit of transactions that can be allowed in accounts opened with form 60.This will further help in ensuring further due diligence of the customer in which more number of transactions can be allowed. Further, Transaction limits on digital channels also can be parameterized based on form 60/PAN details. “Form 60-PAN Applied for” cases can be tracked for obtaining PAN within reasonable time of a month or so.
- Banks are freezing/blocking the accounts based internal triggers, however, as per the Prevention of Money Laundering Act (PMLA), banks do not have the authority to freeze or block customer accounts without proper authorization from a court or Law enforcement agencies (LEAs). In light of this, we may propose this as a suggestion for further consideration by the RBI.

- Bringing all bank cyber teams under one roof to have faster access of freezing the accounts on real time basis on immediate reporting of fraud.

I4C:

- **Hassle Free access to customer:**
  - Allowing customers to access fraudulent I4C portal with hassle free access and minimal inputs and maximum information.
  - Allowing the customers in the respective bank e-platforms with an option to raise a dispute with the transactions and auto reporting to the same to I4C portal in Real-time basis

TRAI:

- Telecom operators provide multiple mobile numbers to the users and RBI permits 6 OVDs for the purpose of CDD. Multiple accounts can be opened with combination of each OVD and with separate mobile number. Recommendations are to be made to TRAI or restriction of multiple mobile numbers to each individual and a cap may be fixed to restrict the inadvertent usage of mobile numbers