Combating mule fraud: Adopting a tech-enabled human-led approach

December 2025

01

Setting the context

In today's digital era, the combination of increased internet access, digital payment systems, global financial integration, and a government-led push for widescale financial inclusion creates a landscape of dual opportunities. While these developments enable swift, real-time transactions anywhere in the world, enhancing user convenience and access to the financial services, they also offer various opportunities for criminals to perpetrate fraud. These fraudsters operate on an unprecedented scale, taking advantage of gullible users to commit fraud, launder money, and engage in other illicit activities.

One of the most prevalent methods involves the use of money mules, who form a part of these systematic and well-orchestrated schemes. Fraudsters adapt their recruitment tactics to align with the potential mule's motivations.[1] These comprise organised criminal groups (OCGs)/money laundering networks (MLNs), which entice, advertise for, recruit, train, incentivise, or coerce individuals into acting on their behalf.

Fraudsters recruit vulnerable individuals such as students, professionals, workers from sensitive areas via online advertisements and get them to open accounts to move illicit funds. Moreover, they directly target financial institutions (FIs) and exploit gaps in due diligence procedures to open accounts using forged or stolen KYC documents.

The growing exploitation of money mules for fraud and the movement of illicit funds is straining the financial ecosystem and eroding trust in FIs, making it imperative to confront and mitigate these challenges.

1.1. Mules: Who are they?

International money laundering watchdog such as Financial Action Task Force (FATF) broadly describes money mules as people who are used to transfer value, either by laundering stolen money or physically transporting goods or other merchandise.

In financial services parlance, the Reserve Bank of India (RBI) defines mule account as a bank account used by criminals to launder illicit funds, often set up by unsuspecting individuals lured by promises of easy money or coerced into participation. The typical features of these accounts, as per the Indian Banking Association,[2] are frequent international transfers, unusually high number of counterparties, rapid transaction velocity, and sudden surges in account activity—which make it difficult to trace and recover the funds.

Money mules can be divided into three main categories: unwitting, wilfully oblivious, and fully aware participants. Unwitting mules do not realise they are part of a criminal operation and often think they are assisting a romantic partner or employer. Wilfully oblivious mules ignore signs of illicit activity in what they're doing—possibly even disregarding warnings from bank staff while opening multiple accounts. Fully aware participants understand their role in the money laundering scheme and willingly cooperate with the broader criminal enterprise.

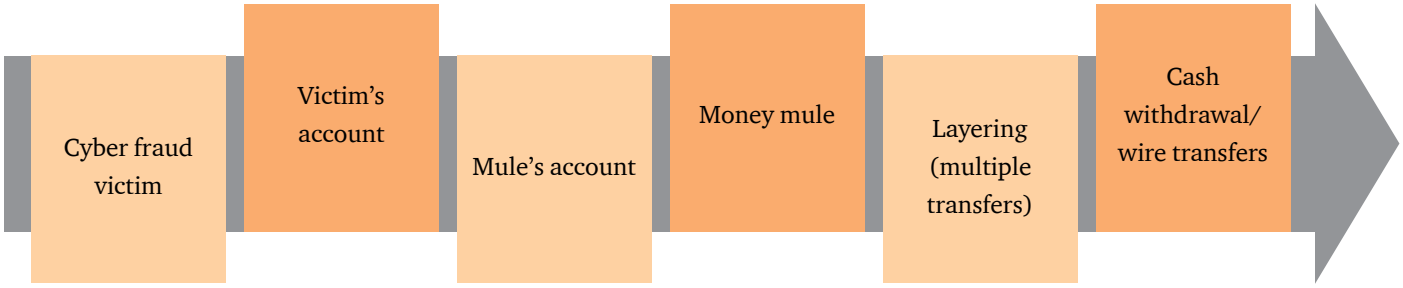
1 FATF Professional Money Laundering – July 2018 - https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf

2 IBA framework to protect the interest of end users from the menace of money mule accounts – January 2025

1.2. Mule operations

Financial services offerings are increasingly digital and global. This shift towards the use of digital solutions like virtual onboarding, real-time transactions, virtual accounts, and digital currencies has created complex chains and increased the ease and speed at which accounts can be created and used by cyber-enabled fraud (CEF) syndicates for money laundering purposes. The proceeds from these criminal activities move rapidly through several transactions, obscuring the stages of money laundering and creating further difficulties for law enforcement to trace and freeze the funds.

Figure 1: Obscuring the trail of money laundering



An in-depth examination of money mule operations conducted by the FATF reveals a strong connection with CEF victims[3] and money mule accounts.

3 FATF illicit financial flows from cyber-enabled fraud – November 2023

1.3. Impact of money mules

While the true volume of money being laundered is difficult to determine, the UN[4] estimated this figure to be $2 trillion, or 2 to 5% of global gross domestic product (GDP). With the ever-growing digitalisation and integration of financial ecosystem, money mules have become the irreplaceable cog in the wheel of money laundering and financial frauds, impacting every nation across the globe.

The Indian Cybercrime Coordination Centre (i4C) projected that the annual loss due to cyber-enabled frauds may exceed ₹ 1.2 lakh crore in 2025, amounting to 0.7% of India's GDP.[5]

I4C also highlighted that in FY24, Indian citizens reported losses of over ₹22,845 crore against cyber financial frauds, with 206% surge compared to FY23.[6] Further, a survey conducted on Indian citizens by Local Circles revealed that 60% of Indians receive three or more pesky or scam calls daily.[7]

It shows that if this menace continues unabated, it will result not only in significant financial losses and mental distress for victims but could also undermine trust in the banking system, adversely affecting sentiments of financial services users and the economy at large.

4 https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html

5 https://www.thehindu.com/sci-tech/technology/cyber-fraud-losses-could-amount-to-07-of-gdp-mha-study-projects/article68788093.ece

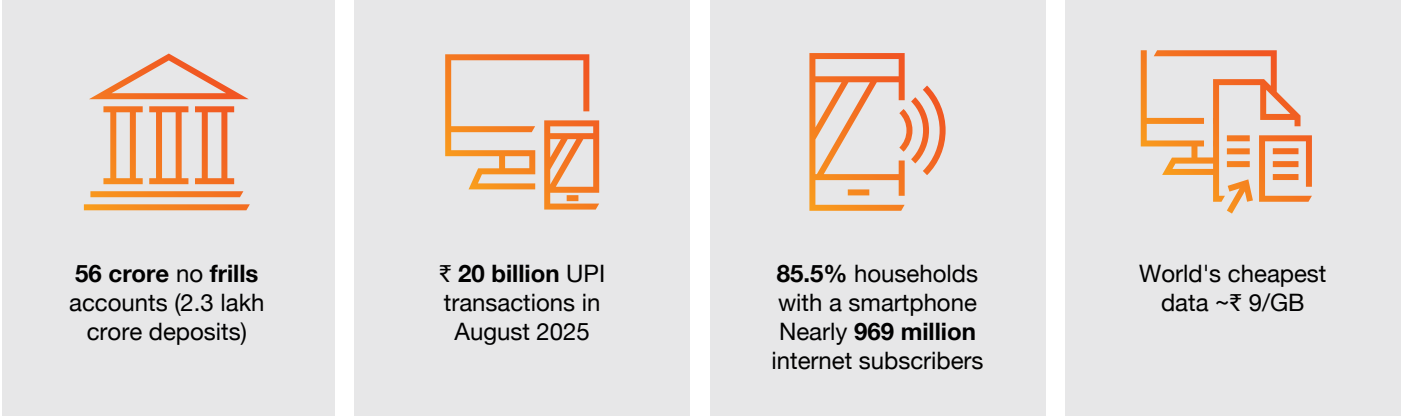
6 https://timesofindia.indiatimes.com/india/indias-cybercrime-reporting-systems-logged-36-lakh-fraud-cases-in-2024-rs-22845-cr-lost-over-10000-arrested/articleshow/122841677.cms

7 https://timesofindia.indiatimes.com/city/pune/fraudsters-feed-on-fears-of-victims-while-many-give-unknown-calls-a-miss/articleshow/116951463.cms

1.4. Why this problem accentuated

In the last decade itself, India has built the world's largest digital biometric identity and real-time payment systems. The key building blocks are the JAM trinity—Jan Dhan (no frills account) + Aadhaar + Mobile—along with technological innovation like UPI and world's cheapest data rates. The use of digital technology has enabled India to achieve financial inclusion for 85% of its population—when only 20% had access to formal banking a decade ago. The National Payments Corporation of India (NCPI) reported 20 billion UPI transactions in 2025 alone.[8]

Figure 2: UPI usage statistics in 2025



This highlights how India's growth in the past couple of decades is closely linked to extending banking services to the remote areas and first-time users of financial services. The RBI[9] has also noted that services like bank accounts, loans, pensions, and insurance—which were once considered luxuries—are now accessible to everyone.

However, while the financial inclusion has advanced, financial and digital literacy have not kept pace. As a result, fraudsters can exploit vulnerable customers by misusing their KYCs and accounts for fraudulent activities and money laundering.

Many individuals, especially those who are new to the digital landscape, lack the knowledge to recognise fraudulent schemes. Common tactics used by fraudsters include phishing, identity theft, and social engineering. These criminals often use sophisticated methods to deceive individuals into sharing sensitive information like KYC details, which are then misused to open unauthorised accounts or carry out illicit transactions.

Exploitation occurs through various means such as fake banking apps, misleading SMS, and emails pretending to be from legitimate financial institutions, and fraudulent calls seeking bank account details under the guise of government benefits or schemes. Once they gain access to personal information, fraudsters can easily siphon off money or use these accounts for money laundering activities, significantly undermining the security and trust in the digital financial system.

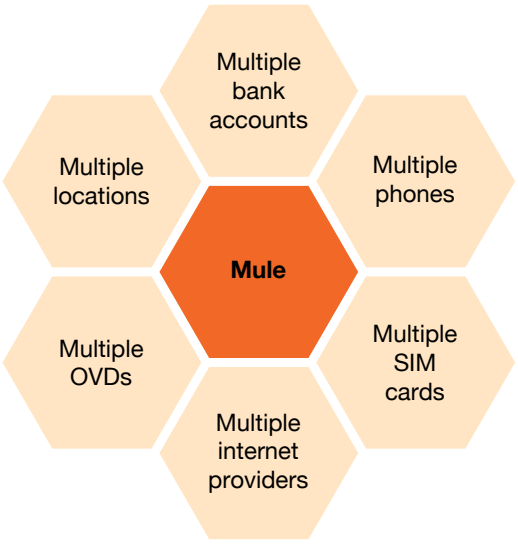
8 https://www.pib.gov.in/FactsheetDetails.aspx?Id=149258

1.5. How mules are exploiting the financial services ecosystem

The digitally enabled and technology driven financial services landscape has created a conducive environment for fraudsters to exploit the non-face-to-face, near real-time nature of banking and financial transactions, making it easier to facilitate money laundering.

Currently, operating a bank account in India only requires a mobile phone and SIM card and any of the six officially verified documents (OVDs) prescribed by the RBI.

Figure 3: How flexible onboarding fuels money mule networks



Consider the scenario in India for opening a bank account. There are 50 scheduled commercial banks, and one can use any of the six OVDs approved by the RBI to open an account. With an Aadhaar card, a person can get up to nine SIM cards. There are no restrictions on mobile numbers, internet service providers (ISPs) or locations. Even with perfect checks in place for KYC verification, account opening, and SIM card or mobile verification, theoretically, a person could manage up to 2,700 savings accounts (by multiplying 50 banks by 6 IDs and 9 SIM cards), plus a multitude of UPI IDs. Although this example might be an exaggeration, as banks usually require Aadhaar for account opening, it shows just how large the scale could potentially grow.

The presence of such alternatives creates opportunities for fraudsters to exploit the banking systems. If banks or law enforcement agencies (LEAs) identify mule accounts and take corrective actions, the fraudster changes course and identifies new opportunities. Some examples are listed in Table 1.

Table 1: Countermeasures by mules against enforcement actions

Action by LEAs/ regulators	Mule's recourse
Block phone/IMEI	Change the mobile phone
Block SIM card/ IMSI	Change the SIM (eight more options)
Block/freeze the account	Change the bank (135 banks)
Block/freeze the OVD	Change the OVD (block Aadhaar, open new account through voter card)
IPs/locations (risk category)	Change the ISPs/location (categorise Jamtara as high risk, he/she will move to Bharatpur)

Due to this dynamic and constantly evolving modus operandi, understanding and monitoring a mule pattern is a challenge for FIs.

9 https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154980&ModuleId=3#:~:text=The%20accessibility%20of%20financial%20services,to%2064.2%20in%20March%202024

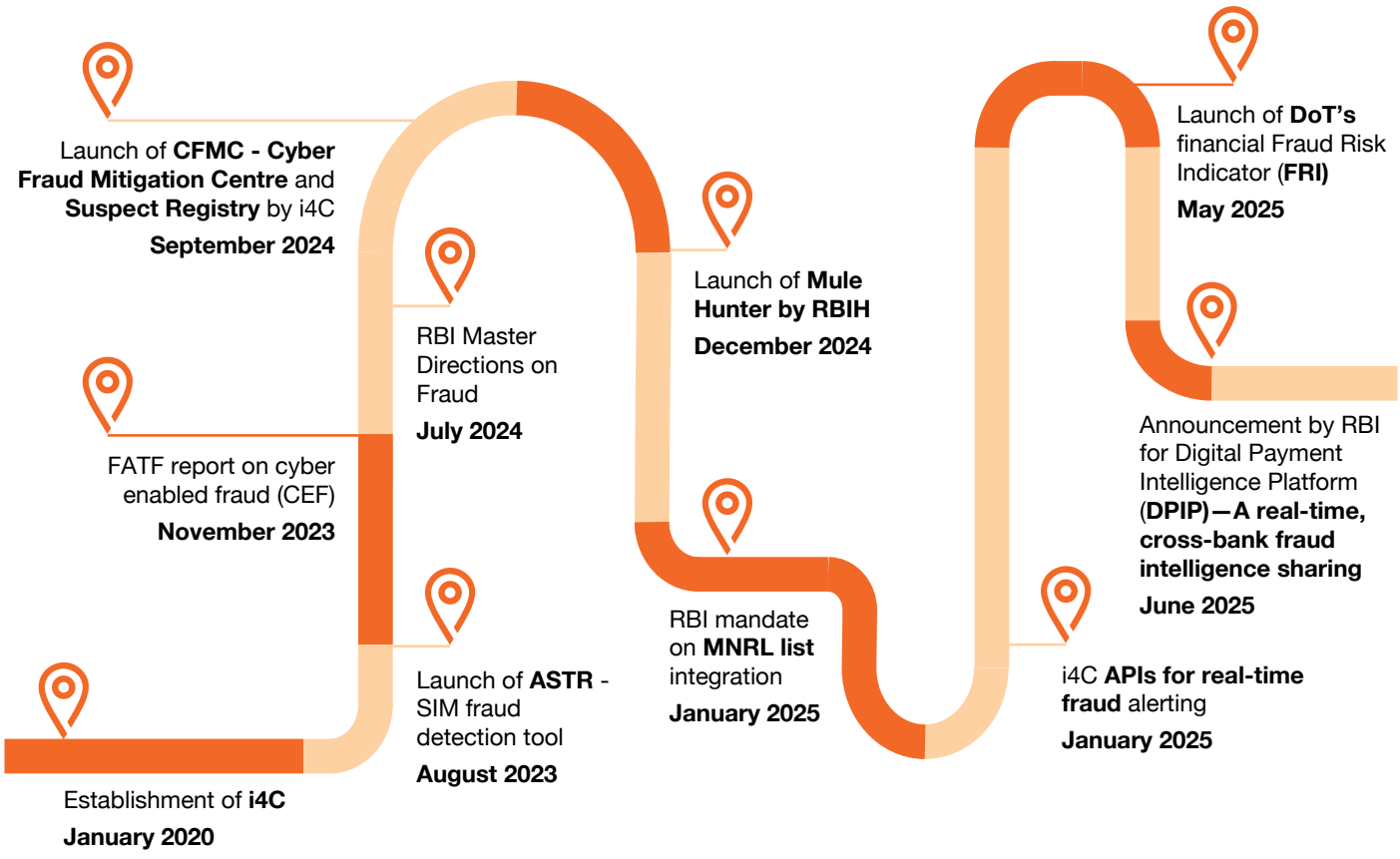
02

Regulatory response and initiatives

Indian regulators have initiated several strategic measures to counter the threat posed by money mules and attempting to address the issue holistically. For instance:

- An MoU has been signed between Financial Intelligence Unit, India (FIU-IND) and RBI for enhanced coordination and information exchange.
- RBI has updated the KYC Master Directions and mandated that banks must strictly follow account opening and transaction monitoring guidelines to detect and act against money mule accounts used for fraud—including timely reporting of suspicious transactions to FIU-IND—failing which non-compliance will be assumed.
- Further, RBI has also developed an in-house AI/ML-based solution Mule Hunter to identify suspected mule accounts.
- The Department of Telecommunications (DoT) has introduced stricter rules for purchasing new SIM cards to curb fraud and protect users. Under these new guidelines, an Aadhaar card is now mandatory for issuing a new SIM.
- The prime minister of India himself raised awareness on mule risks and advised the public to safeguard themselves.

Figure 4: Timeline of key initiatives



While many of these initiatives are yet to yield impactful results across the ecosystem, some of the actions taken are listed in Table 2:

Table 2: Major enforcement measures by regulators to combat fraud

Regulator	Regulatory action
I4C	MHA I4C blocks 9 lakh SIMs; ₹5,500 crore saved in cyber fraud war[10]
	Crackdown on illegal payment gateways PeacePay, RTX Pay, PoccoPay, RPPay[11]
DoT	9.42 lakh SIM cards and 2,63,348 IMEIs are blocked by the Ministry of Communications[12]

Just like these initiatives by the regulators, LEAs are also taking appropriate actions to trace down mule operators.

Table 3: Actions against mule-linked scams

Law enforcement agencies	LEA actions
CBI Operation Chakra V	Uncovered 8.5 lakh mule bank accounts across 700+ branches. Repatriation of 540 Cambodian nationals in scam farms as part of international cyber fraud rings[13]
Enforcement Directorate FIUS Actions – Zara FX Forex Scam	ED raided and froze substantial mule-linked proceeds. The platform used mule accounts to route user funds.[14]
LEAs	A cyber fraud racketeering plot involving mule accounts resulted in a scam amounting to ₹ 175 crore.[15]

As a result of these initiatives, the I4C has reported that 4,000 mule accounts are detected daily, and they have succeeded in preventing approximately ₹4,386 crore from being lost across 13.36 lakh complaints.

Globally, there have been multiple actions and agencies are acting against money mule activities to protect the interest of the customers and safeguard the financial ecosystem. There have been instances where regulators and LEAs have successfully identified mules and enacted appropriate punitive measures against them.

10 https://economictimes.indiatimes.com/news/india/nine-lakh-sims-blocked-rs-5-5k-crore-saved-in-cyber-fraud war/articleshow/ 122866097.cms

11 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2069000

12 https://economictimes.indiatimes.com/industry/telecom/telecom-news/nearly-400k-sims-axed-for fraud/articleshow/123103493.cms

13 https://cbi.gov.in/press-detail/NzA4NA==#:~:text=CBI%20launches%20nation%2Dwide%20searches,Arrest%20under%20Operation%20Chakra%2DV

14 https://enforcementdirectorate.gov.in/sites/default/files/latestnews/Press%20Release%20Search-Zara%20FX-08.08.2025_0.pdf

15 https://www.ndtv.com/hyderabad-news/in-rs-175-crore-hyderabad-sbi-branch-fraud-mule-accounts-used-to-send-money-6439131

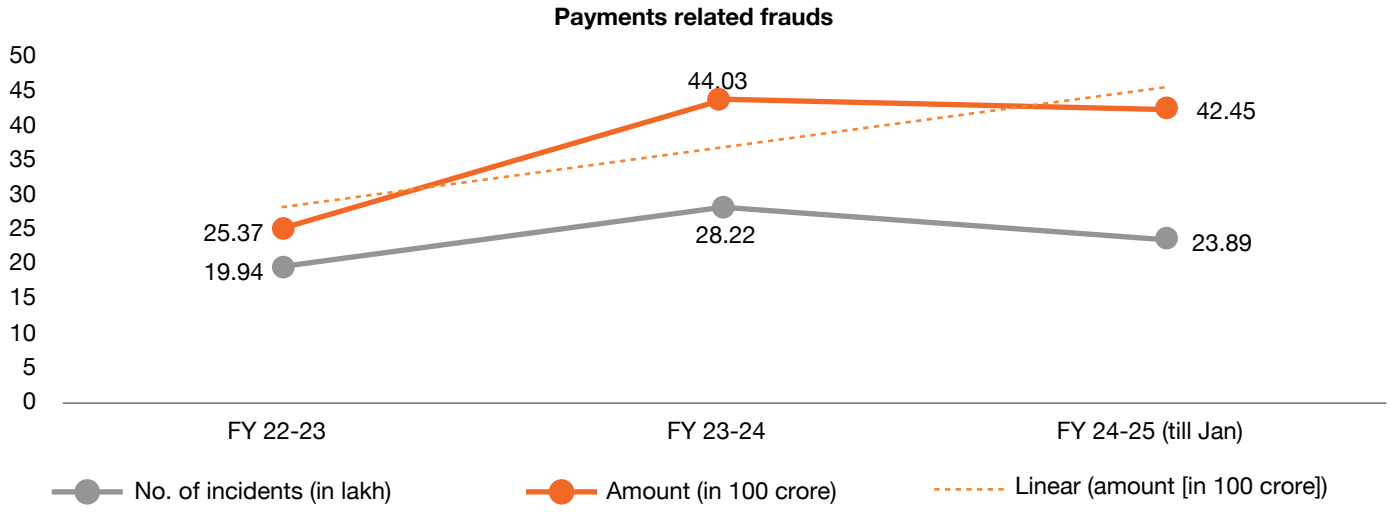
Table 4: Global law enforcement actions against financial crime

Operation/agency	Action
Operation First Light 2024 (Europol, Eurojust, US, UK etc.)	Coordinated international law enforcement crackdowns on online scammers and mule networks; $257 million worth of assets seized[16]
Operation Destabilise (UK NCA + US OFAC)	Unravelled a multi-billion-dollar crypto-based laundering operation[17]

Are these measures adequate?

Our study of rise in cyber frauds and mule activities indicates that governments and regulators have been partially successful in implementing these measures. According to the reports from I4C, in the first nine months of 2024 alone, 1.7 million cybercrime complaints were filed, with losses surpassing ₹11,000 crore. The total cybercrimes reported on Nation Cybercrime Reporting Portal alone witnessed a 42% increase to 22.7 lakh complaints in FY24. Moreover, the RBI has reported that there is a significant rise in digital payments related fraud over the last few years.

Figure 5: Digital financial fraud



Source: https://sansad.in/getFile/annex/267/AU1991_YrbsCv.pdf?source=pqars

This suggests that the problem not only persists but also grows on year-on-year basis. While the government, RBI, FIU, and banks are taking the necessary steps to address this issue, isolated actions are not quite effective. End-to-end mitigation of mule risk requires an integrated approach across the entire spectrum involving regulators, financial institutions, industry bodies and associations, and LEAs—while raising continuous extensive awareness on the issue.

16 https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams

17 https://www.bbc.com/news/articles/c70ezyrep1go

Required regulatory enhancements – Legal provisions

Existing provisions

India currently addresses money mule activities through the Prevention of Money Laundering Act (PMLA), 2002 and various related laws. The RBI through its KYC Master Direction mandates banks to monitor and identify suspicious accounts, including those operated by money mules, and to report such cases to the FIU-IND via suspicious transaction reports (STRs). While these frameworks facilitate the detection and reporting of illicit activities, they do not explicitly criminalise money mule operations.

Limitations of current framework

The absence of a clear, standalone legal definition and explicit penalties for money mule activities limit the effectiveness of enforcement and deterrence of the current rules. Without specific provisions, authorities and FIs must rely on general anti-money laundering (AML) rules, making it challenging to target mule-related crimes directly and comprehensively. This gap hampers swift identification, prosecution, and prevention efforts.

Furthermore, FIs are permitted to block or freeze accounts only upon receiving complaints from LEAs. Even if banks independently identify suspected mule accounts prior to any LEA involvement, they lack the clarity on their authority to take suo-motu actions to block or freeze these accounts for extended periods. Consequently, without explicit provisions supporting such measures, banks are limited in proactively restricting account activity beyond specified timeframes.

Suggested legal and regulatory enhancements

To strengthen the fight against money mule operations, regulators should consider amending the legal framework to explicitly define money mule activities and criminalise their conduct. Clearly articulated penalties (both monetary and imprisonment) and robust enforcement mechanisms will enhance deterrence. Additionally, harmonising guidelines across agencies and fostering industry-wide collaboration will improve detection, reporting, and response capabilities against evolving mule typologies.

Several countries have enacted explicit laws, criminalising money mule activities with defined sanctions, serving as effective deterrents. For instance, the UK and Australia have clear legal provisions under their AML and criminal codes that address money mule offenses, including significant imprisonment terms and fines. Adopting similar targeted regulations in India could reinforce the existing framework and align it with global best practices to combat money laundering more effectively.

Table 5: Jurisdictional treatment of money mule offences and penalties

Country/ jurisdiction	Explicit mule offence – Yes/no	Legal framework/agencies	Penalties for mule activity
UK	**Yes**	POCA, Theft Act, Serious Crime Act; Home Action Plan	Up to 14 years (POCA)
USA	No	Fraud statutes, money laundering laws	Up to 30 years; fines $1 million+)
EU	No	EU AML Directives and national law	Institutional fines (€5 million or 10% turnover)
Australia	**Yes**	AML/CFT Act 2006, AUSTRAC, Criminal Code	Up to 25 years in prison
India	No (via PMLA)	PMLA 2002; RBI KYC/AML	Up to seven years; fines and confiscation

Source: https://sansad.in/getFile/annex/267/AU1991_YrbsCv.pdf?source=pqars

19 Source: Home office Action plan and guidance 2024; AUSTRAC Glossary and Criminal code Act 1995 division 400

03

Existing challenges in effective response to money mules

FIs bear a significant responsibility for detecting and preventing the misuse of the banking ecosystem by money mules and fraudsters. However, they face several structural challenges in establishing a unified front against money mules.

- **Fragmented governance and accountability challenges in combating money mules:** Presently, the responsibilities for identifying and reporting digital fraud and money mule activities are scattered across various departments like compliance, risk, cybersecurity, and analytics. This fragmentation leads to inefficiencies, overlapping or unclear jurisdictions, and lack of coordination amongst various departments. Without a unified strategy, efforts to identify and mitigate fraudulent activities can become disjointed and less effective.
- **Siloed operations:** Identifying money mules often necessitates a detailed analysis of historical transactions as well as real-time action. Traditionally, these responsibilities are managed by separate verticals within the bank—AML (compliance), fraud (risk), and cybersecurity. This division has led to delayed actions and impede effective detection and prevention. For instance, few banks are implementing the FIU Cyber Enabled Fraud Red Flag Indicators—which are primarily developed to address money mule related frauds—in AML transaction monitoring system while the others are developing them in Enterprise vide Fraud Risk Management solution.
- **Challenges in KYC operations and onboarding:** Digital onboarding poses risks, as it requires seamless integration between multiple verification sources, such as PAN, Aadhaar, voter card and mobile verification, which complicates the process. Post-onboarding operations require continuous monitoring against evolving threats and the dynamic nature of customer interactions, changes in customer information, such as address or contact updates. The processes are being misused to mask underlying fraudulent and money mule activities.
- **Delay in response:** Most banks currently take up to 30 days to respond to police inquiries, while the critical window to intercept swindled funds, often referred to as the 'golden hour', is just two hours.[18] Real-time information sharing across the financial sector at various forums, such as suspect registry and FRI list, is needed to reduce the response time against mule activity.
- **Challenges in external data integration:** Data from diverse sources, such as the I4C suspect registry, MNRL list, CFR, and CPFIR tend to be fragmented and inefficiently utilised. Current tools often lack the capability to directly consume and apply these data sources. Few banks are blacklisting or grey listing the details while others are integrating them in onboarding applications. Resources lack understanding as to how to integrate, leverage, and investigate alerts generated basis these lists.
- **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 rigid threshold values, oversimplified approach to designing of rule engines, and dependency on qualitative inputs like customer behaviours, device signatures etc. to design the detection systems.
- **Technology constraints and AI/ML models:** Real-time solutions yield high false positives and customer complaints, while traditional non-real-time solutions cause delayed responses against money mules.
- **Limited post-identification actions on suspected mule accounts:** When a bank suspects an account of being used as a mule, it conducts enhanced due diligence (EDD). Based on this, there are four possible scenarios with corresponding actions (example in Table 6).

18 https://www.thehindu.com/news/national/karnataka/casinos-to-crypto-how-cybercriminals-launder-money/article69899023.ece

Table 6: Enhanced due diligence on suspected mule accounts and probable outcomes

Account	KYC checks	Source of funds	Transaction patterns	Mule activity	Action taken
1	Positive	Positive	In line with profile	Unlikely	No action
2	Positive	Positive	Not in-line with profile	Likely	STR filing
3	Positive	Negative	Not in-line with profile	Highly likely	STR filing, block/freeze
4	Negative	Negative	Not in-line with profile	Very high likelihood	STR filing, block/freeze, terminate account-based relationship

1. **Account 1:** KYC and source of funds are positive, and transaction patterns align with the customer profile. Mule activity is unlikely, so no action is taken.
2. **Account 2:** KYC and source of funds are positive, but transaction patterns do not align with the profile, indicating likely mule activity. Banks may choose to file an STR.
3. **Account 3:** While KYC is positive, the source of funds is negative, and transaction patterns are inconsistent with the profile, making mule activity highly likely. Banks may file an STR and temporarily freeze the account. However, they lack the clarity on their authority to block or freeze such accounts beyond a limited timeframe since the accounts remain KYC-compliant.
4. **Account 4:** Both KYC and source of funds are negative, and transaction patterns do not match the profile, indicating a very high likelihood of mule activity. Banks are able to file an STR, freeze the account for extended periods, and terminate the customer relationship.

Due to the absence of explicit legal or regulatory provisions and the required clarity for handling cases like Accounts 2 and 3, banks face challenges in taking swift, decisive, and uniform actions. This results in varied practices adopted across banks in managing suspected mule accounts under these circumstances.

Fraud function vis-à-vis AML function

The fundamental driver for all the above challenges lies in how the AML and fraud functions have been aligned within the bank. Historically, due to the disparate nature of their operations, AML and fraud functions have primarily organised themselves into compliance and risk functions respectively. This separation has been reflected in the governance, operations, tools, and technologies leveraged by these functions.

The AML function has traditionally been viewed as a retrospective operation, with tools aligning with this post-facto approach, focusing on suspecting customers. In contrast, within a digital environment, the fraud function primarily focuses on prevention—protecting customers from frauds such as account takeovers, identity theft, stolen login credentials, business email compromises, phishing, and vishing attacks. Consequently, the tools and technologies fraud functions adopt are geared towards real-time prevention and detection.

Table 7: Governance structure vs resulting gaps—money mule risks

Area	AML (compliance vertical)	Fraud (risk vertical)	Resulting gaps
Mandate	Regulatory compliance, STR filing, transaction monitoring	Scam prevention, account takeovers, fraud detection	No shared accountability for cross-cutting risks like money mules
Focus	Suspects customers for money laundering	Protect customers from fraud risks	Challenging to stop mule transactions in real time
Objective	Detects laundering through unusual transaction patterns (FIU – RFIS)	Prevent and detect fraud and resulting financial loss	Disconnect between behavioural scam patterns and AML red flags
Tools and technology	**Post facto**; rule-based transaction monitoring solution, name screening	**Real-time** risk scoring, device fingerprinting	No integrated alerting or joint case investigations
Alerts	Threshold breaches, name match, risk-based monitoring	Behavioural anomalies, login/IP/ device mismatch	Split view of money mule risks – same ID may be flagged for fraud and AML teams both
Data requirements	Focus on transaction data; KYC data for name screening	Non-financial data; behavioural anomalies, login/IP/ device	Detecting mules requires both historical transaction data as well as non-financial data and real-time behavioural anomalies
Regulator	FIU-IND	RBI	Inconsistent policies – FIU mandates to not ‘tip-off’ the customer; RBI mandates to monitor in real time

Money mule operations have put a spotlight on this segmentation and how banks are handling these challenges. Since money mules act as intermediaries who facilitate the flow of illicit funds derived from fraud, they essentially bridge the gap between fraud detection and AML measures.

The complex interaction between mules and fraud victims calls for a unified approach within financial institutions. To address this, banks need a collaborative and integrated approach to tackle fraud prevention, intelligence and AML compliance, ensuring that responsibilities are carried out effectively.

04

Building a resilient framework against money mule fraud

4.1 Senior leadership sponsorship and commitment

Senior leadership commitment and sponsorship is critical for the success of the money mule mitigation framework. This includes investing in integrated technologies that bridge gaps between different systems, facilitating seamless data utilisation, and enabling real-time risk analysis with refined AI/ML models. Leadership should also advocate for the refinement of rule-based systems to detect threats more accurately, thereby reducing false positives and improving resource efficiency. By fostering a culture of collaboration and continuous innovation, senior leaders can empower their institutions to form a cohesive strategy that effectively combats the threats posed by money mules.

4.2 Framework for an integrated approach

An integrated approach to money mule risk mitigation combines end-to-end bank controls with ecosystem collaboration—enhancing onboarding and KYC, cross-channel transaction monitoring, behavioural analytics, risk-based models complemented by external intelligence, and information from FIs, LEAs, and the card network.

However, to achieve this, Fis should first address any inherent challenges by performing a discovery and diagnostic of current state as highlighted in Figure 6.

4.2.1 Discovery and diagnostics

Figure 6: Key tenets of an integrated approach to money mule mitigation

Shared responsibility

- Shared but clearly defined responsibilities between EFRM/AML and intelligence teams
- EFRM for alert generation and AML for investigations
- Leverage EFRM layer for decision matrix for real-time block/freeze and AML for STR reporting

01

Data quality and insourcing

- Insource device/IP/KYC/transaction data in a unified layer in DWH/data lake
- Create derived schemas required for effective ML features/rule creation
- Insource external data for configuration

02

Tools and technology

- Configure known mule patterns as rules
- Leverage ML models for anomaly detection and new typologies and complex patterns
- Integration with fraud streaming layer for real-time block/freeze decision matrix
- Network link analysis

03

External source integration

- Integrate with **MNRL list** in the onboarding channel. Periodic screening with existing data files
- Integrate with **suspect registry**, bifurcate the information to be consumed by EFRM/AML/ onboarding teams
- Leverage **FRI** indicator

04

Unified case manager and decision matrix

- Have a unified case manager for investigations
- A decision matrix for information sharing and consumption, which is to be configured in channels, EFRM system or as a rule
- Limit bulk pay-out services, restrict VPA creation

05

Investigation and awareness

- Reduce TAT and redundancy
- Configure checks on onboarding applications
- Create specialist AML/fraud teams for mule typologies (romance/investment scams, etc.)

06

To effectively leverage this integrated approach, banks need to:

- Address data quality issues and align fragmented data such as device, IP and geographical signatures, as well as customer behaviour, transactions and KYC profiles—which are often available on different source systems and channels.
- Leverage both rules for known patterns as well as ML models to identify new and complex patterns. However, the effectiveness of mule detection via rules or ML models depends on the quality of features and variables derived from various data sources.
- Have a unified intelligence layer to collate and consume data from internal and external sources and provide a holistic view of customers, accounts, transactions, entities, and devices.
- Have a unified case manager to optimise resources, reduce duplication, and provide a consistent view of mule-related risks.
- Enable real-time monitoring and interdiction to stop suspicious transactions before funds exit the ecosystem, especially where mule accounts act as transient pass-throughs.
- Integrate external intelligence feeds (such as consortium data, watchlists and industry-shared mule markers) to enrich detection beyond internal systems.
- Continuously update detection strategies by incorporating feedback from investigations, law enforcement, and evolving typologies into updated features and rules.
- Prioritise feature engineering and explainability so that variables derived from analytics (e.g. device clusters, transaction velocity shifts, cross-channel correlations) are transparent and can be trusted by investigators and regulators.
- Incorporate temporal analytics to capture short-lived patterns typical of mule accounts, such as sudden bursts of inflows followed by rapid withdrawals.
- Leverage cross-entity analytics that look at households, shared infrastructure or connected accounts, instead of analysing customers in isolation.

To complement the integrated approach outlined above, Table 6 presents a structured framework for money mule prevention, detection, and response. This framework highlights specific strategies across people, processes, and technology to effectively address mule account activities at various stages.

Table 8: Framework for combat mule account activity

Area	Prevention	Detection	Response
Technology and transaction monitoring	• Risk-based transaction rules (velocity, layering patterns) • IP/device tracking, proxy/VPN flagging	• AI/ML models to detect funnel accounts • Common IP/device clustering	• Real-time blocking of funds • Flag to internal fraud/AML teams
Data models integration	Leverage external data sources for effective configuration at the time of onboarding and continuous monitoring	Leverage external sources for rules and features for ML models	Enrich central database of I4C, RBI with proactive updates
Customer awareness and communication	• Public campaigns by the banks • RBI Kehta Hai	• Flag customers with repeated risky behaviour	• Contact customer with warnings • Deactivate/freeze mule accounts • File reports to LEAs
KYC/CDD/EDD controls	• Screen for fake/forged documents • Prevent use of synthetic ID and mule recruitment abuse • Configure checks on onboarding applications	• Revalidate KYC after sudden changes (email, mobile, address, etc.)	• Offboard mule customers • Report suspicious updates to FIU/LEAs/I4C
Employee and agent awareness	• Train staff to identify mule signs (e.g. student or unemployed with large inward funds)	• Internal alerts when frontline staff raises onboarding concerns	• Escalate to fraud ops/ compliance • Document for audit trail
Investigation/ forensics	• Create specialist AML/fraud teams for mule typologies (romance/ investment scams, etc.)	• Network link analysis of transactions, accounts, beneficiary mapping	• File SAR/STR • Coordinate with law enforcement/cybercrime
Account and channel controls	• Limit bulk payout services • Restrict VPA creation, third-party wallet linking in high-risk current accounts	• Flag sudden changes in account usage or login IPs • Monitor account cross-access patterns	• Freeze suspicious accounts • Notify other banks via LEA or industry coordination
Reporting and escalation	• Mandatory mule indicators in internal SOPs for STR generation	• Automated STR/SAR flagging based on mule red flags	• Submit STRs to FIU-IND, freeze accounts
Third-party (merchant/ FinTech)	• Merchant onboarding screening for drop/mule accounts • Educate FinTechs on misuse risk	• Track merchants with high refund/payout ratios	• Suspend relationships with mule-linked merchants or PSPs, freeze accounts

The above discovery and diagnostic of current state will help FIs to translate their framework into an actionable technological solution—an integrated technology layer.

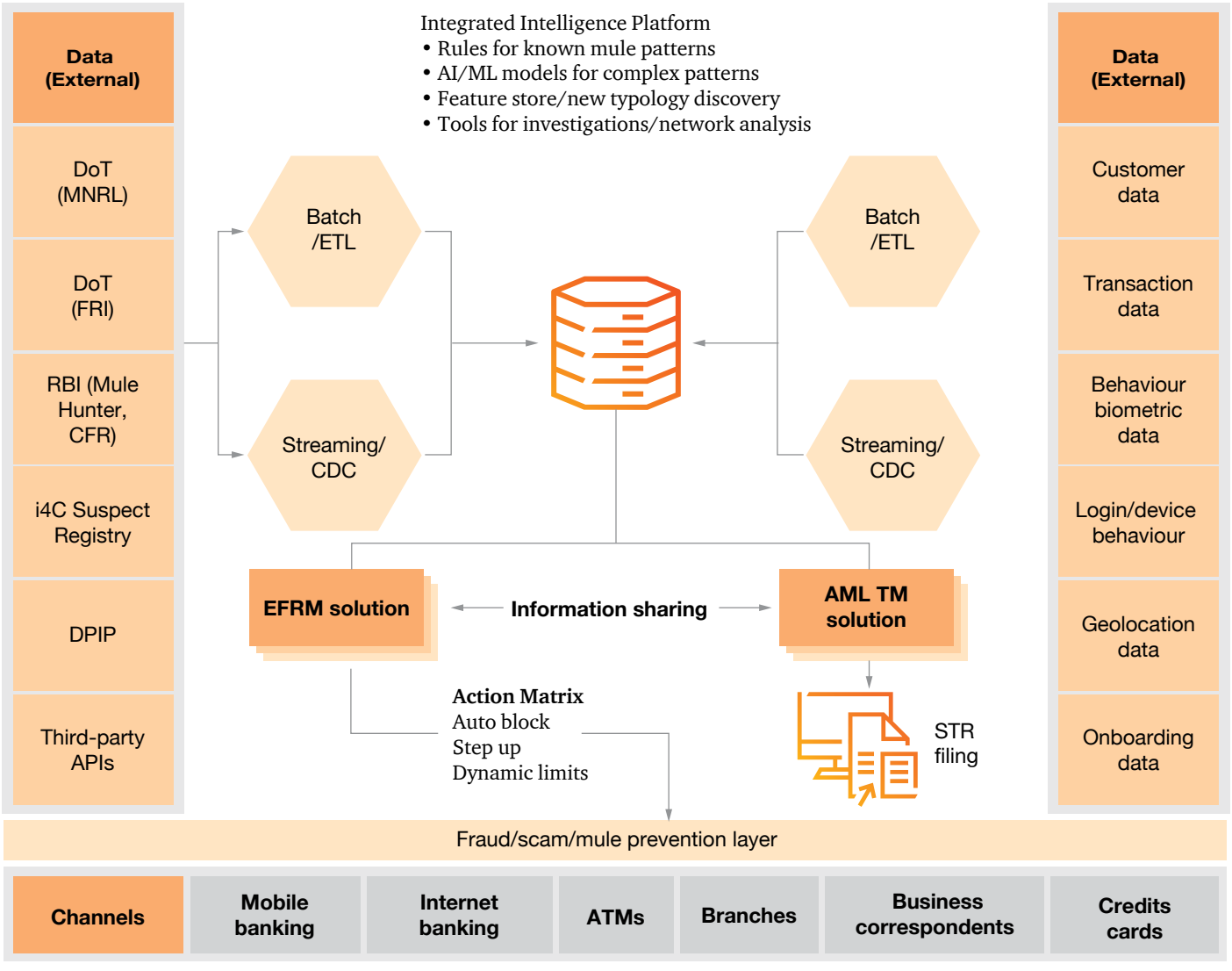
4.2.2 Integrated tech layer for mule detection and response

The effectiveness of prevention and detection measures heavily relies on the availability of data and technology, as well as the capacity of financial institutions to design, customise, and integrate these elements for optimal outcomes. It involves creating a technology stack and underlying scalable IT infrastructure to act as a backbone for implementing the integrated approach.

The integrated tech layer should integrate diverse data sources such as transaction data, KYC information, and external data lists into a centralised data mart, and it should provide a 360° view of customer and device activities. By integrating AI/ML and advanced data management techniques, the proposed architecture should not only harness rule-based detection and supervise ML models to discover anomalies but also employ advanced typology discovery for detecting unknown and emerging money mule patterns. Decision engines and orchestration layers utilise these insights for real-time threat evaluation, enabling actions like account blocking or initiating extra verification steps.

The overall architecture for an integrated solution may include the following layers:

Figure 7: Architecture for mule account detection and response solution



- The ‘Channels and source data’ layer gathers information through various onboarding methods and processes including vKYC/eKYC, mobile and web applications, payments and external sources—such as negative lists, suspect registries, LEA requests, known mule accounts and high-risk locations. This data serves as the foundational input for identity resolution and analysis.
- Once collected, data is fed into an ‘integrated intelligence platform’, creating detailed Customer 360 and Device 360 profiles using deterministic keys like PAN, masked Aadhaar, mobile numbers and device hashes, alongside probabilistic matching techniques such as names, DOBs, and fuzzy addresses. These comprehensive profiles help fraud ops teams engage efficiently with customers and help AML teams in making STR decisions.
- The ‘intelligence platform’ develops a feature store with both online and offline elements. It incorporates behavioural factors like device/account-first appearances and geolocation variance, transaction flow factors like rapid pass-through, and graph-based analyses like shared device across accounts. These datapoints are used in building supervised models and anomaly detection mechanisms, providing crucial information to a decision engine. Finally, decisions are categorised based on the pattern recognition results.
- High probability mule patterns are handled quickly by the action matrix, whereas cases requiring in-depth evaluation by AML analysts culminate in STR filing decisions. This approach emphasises the advantages of the integrated approach in managing money-mule risk. By utilising advanced profiling and ML, coupled with swift decision-making, the system effectively mitigates risks with minimal disruption in the bank’s existing architectural setup. This approach allows banks to enhance their mule risk mitigation capabilities while maintaining operational continuity and stability.

05

Conclusion

The growing challenge of money mule operations within the financial ecosystem emphasises how these schemes exploit individuals and systems to facilitate money laundering and commit fraud. The continuous rise in cybercrimes indicates that isolated actions are insufficient in addressing this issue effectively.

To reach maturity in mule risk mitigation, organisations must invest in an integrated approach, refining their rule-based systems and enhancing AI/ML capabilities. This includes cultivating a culture of collaboration between fraud, risk and compliance teams, ensuring coordination and sharing of insights across departments. Moreover, financial institutions should prioritise continuous improvement and updates in system technologies to reduce false positives and improve real-time threat detection accuracy. Sponsorship by senior leadership and adherence to a strategic governance structure, while fostering education and awareness among staff, further support a well-rounded and proactive risk management environment.

Finally, at the ecosystem level, addressing the mule threat requires collaborative efforts among multiple stakeholders, including regulators, financial institutions, LEAs, industry associations, and the customers. By encouraging information sharing and establishing standard protocols for detecting and reporting suspicious activities, the ecosystem can efficiently tackle the mule phenomenon. Collective efforts in unifying approaches and deploying integrated security measures across organisations will drive overall improvements in the financial ecosystem's resilience against ongoing and future mule-related threats. Enhanced communication, awareness campaigns and technological innovations can collectively neutralise the influence of money mules and safeguard the interests of all parties involved.

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.
Please see www.pwc.com/structure for further details.

Contact us

Siddharth Vishwanath
Partner and Leader - Risk Consulting
PwC India
siddharth.vishwanath@pwc.com

Minaar Malse
Partner and Leader - Risk Consulting Financial Services
PwC India
minaar.malse@pwc.com

Puneet Garkhel
Partner and Leader - Financial Crime and Compliance, Risk Consulting
PwC India
puneet.garkhel@pwc.com

Dhruv Chawla
Partner - Financial Crime and Compliance, Risk Consulting
PwC India
dhruv.chawla@pwc.com

Induvant Tomar
Executive Director - Financial Crime and Compliance, Risk Consulting
PwC India
induvant.tomar@pwc.com

Contributors

Rajeev Kumar Singh, Brahmadev Sharma

pwc.in

HS/November 2025 - M&C 49120