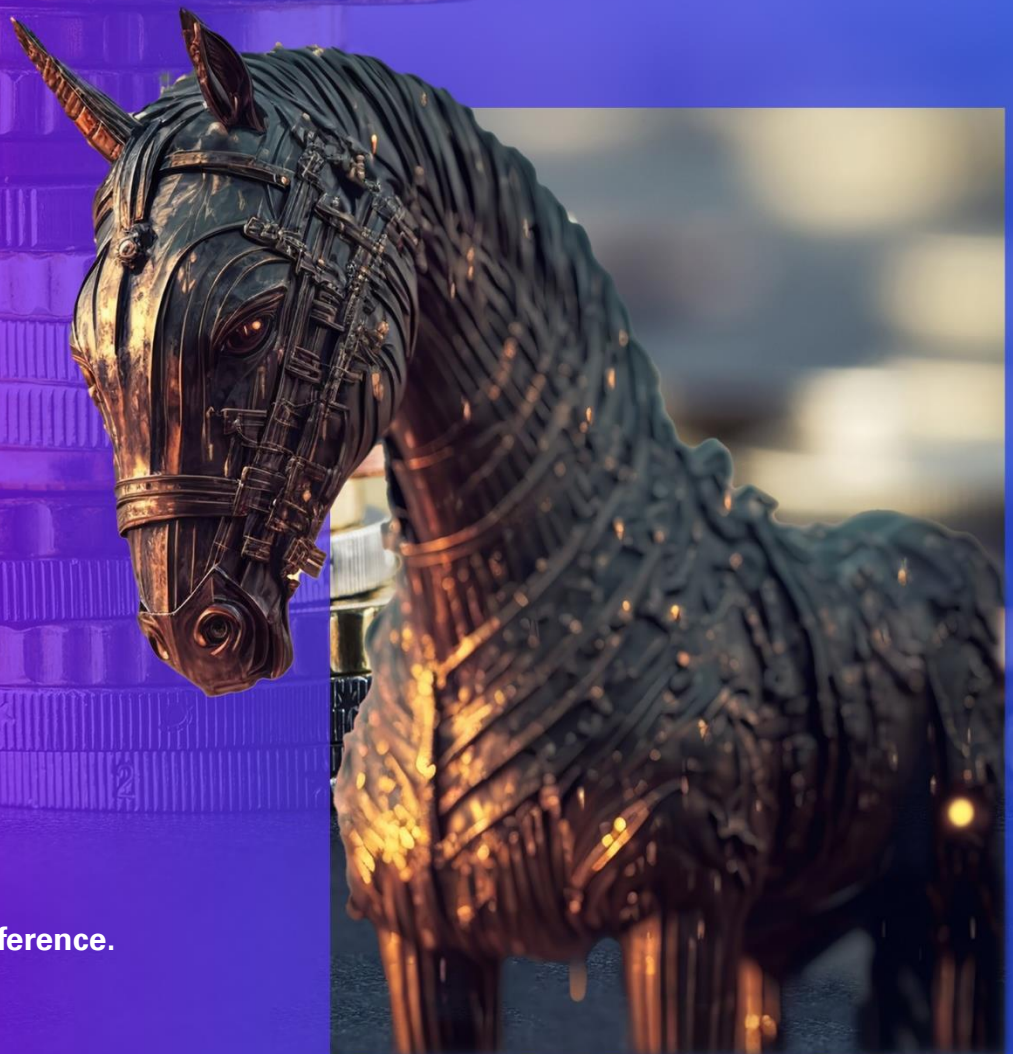




Money Mules: FinCrime's Trojan Horse Unveiled



kpmg.com/in

KPMG. Make the Difference.

Setting the context

Originating from the ancient Trojan deception, Money Mules embody a modern-day Trojan horse strategy, deftly navigating through complex digital financial systems. Their primary role? To mask the origins of illegal funds under a pretext of legitimacy. Much like the naïve Trojans who welcomed the wooden horse within their citadel, individuals lured into money muling unwittingly step into a convoluted web of financial fraud.

In today's digital age, this tale of deception serves as a stark reminder of the lurking perils beneath seemingly routine financial transactions. The continuous evolution of the digital space amplifies these risks, demanding heightened vigilance and proactive measures. As financial criminals innovate, awareness and robust safeguards become imperative shields against this invasive threat.

"Money Mules" or "Mules" are individuals who knowingly or unknowingly assist in transferring illegitimate funds, making them appear legitimate. Criminals may recruit Money Mules and use their genuine accounts to launder illicit money during the layering stage, where funds are moved to conceal their illegal source. Later, mules deposit money into the financial system by transferring funds between accounts, and return the layered funds back to the criminals, making it challenging for law enforcement to trace the money trails.

1. Placement:

Illicit funds introduced into the financial system

3. Integration:

Integrate illicitly obtained funds into the legitimate financial system

2. Layering:

Money transferred through a series of transactions to conceal its origin often involving 'Money Mules'





What has triggered a sudden rise in Money Mules?

The digitisation of payments and transactions is evolving rapidly, with organisations and customer embracing digital payment channels for transmitting and receiving money. In India, the digital payment volumes have witnessed an average growth rate of 50 percent over the past five years, indicating a paradigm shift to online financial transactions from traditional cash-based transactions¹. While this evolving landscape has brought unparalleled convenience, it has also paved the way for a concerning trend - increased financial crime risk, which includes emerging risk typologies such as Money Mules. In 2016, the Reserve Bank of India (RBI) had warned banks of misuse of Jan Dhan² accounts by Money Mules³.

Financial Institutions including banks, payment firms, money service bureaus, etc. have been a victim of significant mule operations in recent times. Mule operation has been increasing due to a combination of factors including economic uncertainties, technological supremacy, and tech savvy criminals. Some key factors that may have attributed to its meteoric rise are listed below:

Increased Cyber threats

Growth in cyber threats, including phishing, malware attack, and data breaches lead to compromise of customer accounts resulting in scams. Money Mules are often recruited to assist in laundering illicit funds obtained from these scams.

Digital banking boom

Digital banking platforms have made bank account opening and fund transfer seamless. With the adoption of Unified Payments Interface (UPI), fund transfer happens in fraction of a second. This has increased transaction volume, making way for perpetrators to indulge in increased criminal activities like mule operations.

Economic uncertainties

Global economic uncertainties across the globe may act as a trigger in rise of mules as it facilitates quick and easy money. Students studying abroad, and unemployed youths needing quick money are softer targets for these scams.

Sophisticated Fraud Schemes

Criminals employ sophisticated fraud schemes, such as Authorized Push Payments (APP), Business Email Compromise (BEC) and Account Takeover (ATO), to gain unauthorized access to bank accounts or manipulate legitimate transactions. Money Mules play a role in facilitating the movement of illicit funds, making it harder for FIs to detect and prevent fraud.

Technological Growth

Rapid technological advancements such as cryptocurrencies, blockchain, Generative AI and Large Language Models, etc. has contributed to increased challenges for law enforcement agencies in tracking cross-border illicit transactions, thereby making activities such as Money Mules thrive.

Lack of awareness and education

Lack of public awareness especially among young adults and older generation could be a contributing factor to this problem. Regulators across the globe have recognised this as a significant problem and have started playing a pivotal role in creating public awareness to safeguard citizens.

1. Revealing Risks in India's Financial Landscape: Exploring AI-Driven Detection of Mule Accounts, Reserve Bank Innovation Hub, April 2024
2. Pradhan Mantri Jan Dhan Yojana is a financial inclusion program launched by the Government of India in 2014 for Indian citizens, that aims to expand affordable access to financial services such as bank accounts, remittances, credit, insurance, and pensions.
3. Jan Dhan accounts more vulnerable to frauds: RBI, Economic Times, May 2016.

Indian Regulatory Landscape

The Indian regulatory landscape for money mule activities falls under the purview of the Prevention of Money Laundering Act (PMLA), 2002; regulations issued by the RBI and guidelines issued by the Financial Intelligence Unit – India (FIU-IND).

- As part of regulatory actions taken by Reserve Bank of India (RBI), a circular dated 7 December 2010 was issued on 'Operation of bank accounts and Money Mules' stating, "Money Mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "Money Mules."⁴
- On October 17, 2023, RBI amended the Master Direction — Know Your Customer (KYC) Direction, 2016, signaling an emphasis on combating money laundering involving Money Mules. The amendment stated that "Banks shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no Suspicious Transaction Report (STR) was filed by the concerned bank, it shall then be deemed that the bank has not complied with these directions."⁵
- Money mule is a key emerging insidious threat and basis the National Crime Records Bureau (NCRB) data, online financial frauds constituted a staggering 67.8% of all cybercrime complaints received in Q2 2022⁶.

Global regulatory landscape

The global regulatory landscape around Money Mules involves key regulations, aimed at preventing financial crimes, especially money laundering and terrorism financing.

- The UK's Financial Conduct Authority (FCA) published an article 'Proceeds of fraud - Detecting and preventing Money Mules'⁷ in October 2023, providing a deep dive on current good practices followed by financial institutions and areas of improvement in detecting and preventing Money Mules.
- The Hong Kong Monetary Authority⁸(HKMA) has created a robust and comprehensive framework for combating financial crimes due to money laundering including a legal framework, preventive measures basis risk-based approach and effective strategies by law enforcements. It encourages banks to adopt Regtech in AML, especially for detecting mule account networks related to fraudulent activities.
- In April 2023⁹, Singapore's Ministry of Home Affairs (MHA) and the Smart Nation and Digital Government Office (SNDGO) proposed stricter laws to strengthen the country's defense against scams facilitated by Money Mules. Proposed amendments to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) (Amendment) Bill (CDSA Bill) and the Computer Misuse (Amendment) Bill (CMA Bill) that would hold Money Mules criminally liable for their actions.
- The European Union's Fourth Anti-Money Laundering Directive (4AMLD) and Fifth Anti-Money Laundering Directive (5AMLD) aims to strengthen AML regulations by expanding the scope of covered entities and enhancing transparency requirements. In November 2022, law enforcements from 25 countries supported by Europol, Eurojust, INTERPOL and the European Banking Federation (EBF) joined hands as part of an operation named 'European Money Mule Action 2022' to crack down on Money Mules and their recruiters.

4. Operation of bank accounts and Money Mules, Reserve Bank of India, December 2010.

5. Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on January 04, 2024), Reserve Bank of India

6. Proceeds of fraud - Detecting and preventing Money Mules, Financial Conduct Authority, November 2023

7. Revealing Risks in India's Financial Landscape: Exploring AI-Driven

Detection of Mule Accounts, Reserve Bank Innovation Hub, April 2024

8. Preventing bank accounts from being used for money laundering, Government of Hong Kong dated 06 December 2023

9. Tougher laws passed to clamp down on Money Mules, sale of Singpass and bank accounts, Straits Times, May 2023

10. 2 469 Money Mules arrested in worldwide crackdown against money laundering, Europol, 2022



A snapshot of key highlights of 'European Money Mule Action 2022':

European money mule action 2022

Combined efforts by law enforcements from various countries helped crack down on one of the most important enablers of money laundering - Money Mules and their recruiters

8,755

Money Mules were identified

1,648

Investigations were initiated which was supported by around 1800 financial institutions from 25 countries

EUR 17.5 million

prevented from being laundered by Money Mules in three-month action

222

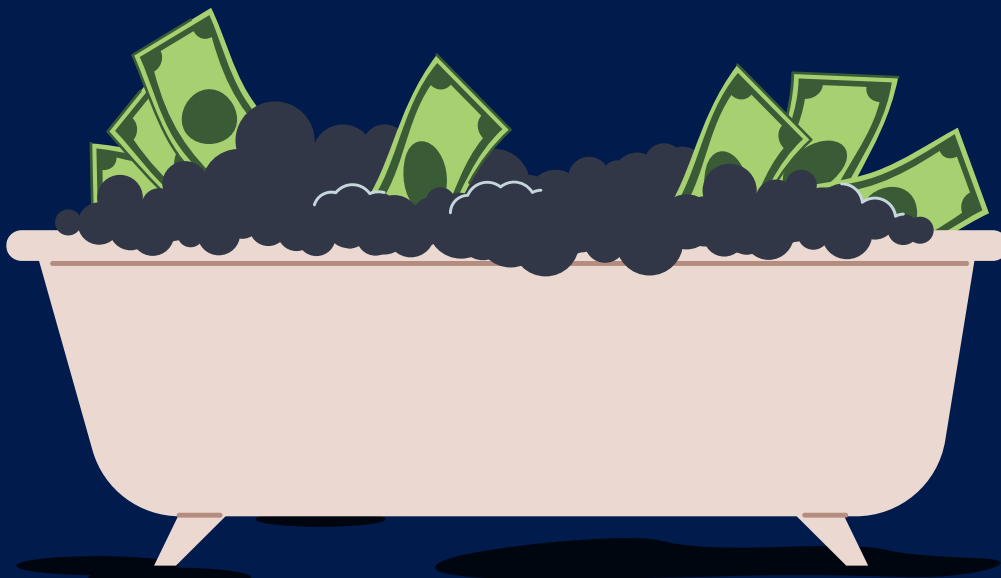
money mule recruiters were identified

4,089

Fraudulent transactions were identified

2,469

individuals were arrested worldwide





Categories of Money Mules

In the contemporary landscape, diverse types of Money Mules can be identified, spanning from unwitting individuals deceived into illegal operations to complicit ones who are fully cognisant of their participation in such activities. Financial Institutions (FIs) including banks must monitor for these individuals to prevent money laundering activities and protect the integrity of the financial system.

Money laundering technique using Money Mules is similar to Smurfing as the modus operandi of both involves breaking amounts into multiple small transactions to avoid detection, but differs in as much as the former (Money Mules) often involve unaware individuals who unknowingly or unwittingly facilitate the laundering, whereas in smurfing the launderer's own (shell) entities/bank accounts are used.



Unwitting money mule

- Individuals are unaware about their involvement in criminal/illegal activity
- Manipulation of victim for granting access to their account for receiving/transferring money
- Targeted through advertisement about fake online jobs, posts on social media platform or scams such as job scam, romance scam, phishing/smishing/vishing scam, investment scam or lottery scam



Witting money mule

- Individuals are partially aware about their involvement in suspicious or illegal activity
- Individual may be under pressure, motivated by financial gain or have ignored clear red flag indicators
- Individuals are willing to accept the risk involved in the movement of funds



Complicit Money Mules

- Individuals are fully aware about their involvement in criminal/illegal activity
- Intentionally a bank account is opened for receiving and transferring illicit funds. Further, they may be aware about the individuals involved in money laundering activities
- Might be engaged in recruitment of other Money Mules





Lifecycle of money muling

The risk of legitimate users granting access of their account to fraudsters is much higher as compared to bank accounts directly opened by the fraudsters for illicit movement of funds. The entire lifecycle of a money mule operation is divided into multiple stages starting from recruitment of the mule. The below picture depicts the end-to-end cycle of a mule operation:

Initial Transaction:

The recruited individuals, known as Money Mules, are instructed to provide their bank account details or open new accounts to receive funds obtained through illegal activities such as phishing scams, identity theft, or fraudulent transactions

Layering:

To obscure the trail of the illicit funds, Money Mules engage in a series of complex transactions, including multiple transfers between accounts, conversions into different currencies, and purchases of assets or goods, making it challenging for law enforcement to track the money's origin

Monitoring:

Criminal organisations closely monitor the activities of Money Mules to ensure that the laundering process proceeds smoothly and that law enforcement detection risks are minimized

Recruitment:

Individuals are recruited, often through online job postings, social media, or direct contact, with promises of easy money or legitimate job opportunities. They may be unaware of the criminal nature of the operation

Money Transfer:

Once the funds are deposited into the mules' accounts, they are instructed to withdraw the money in cash or transfer it to other accounts, often overseas, using various payment methods such as wire transfers, cryptocurrency, or prepaid cards

Integration:

Such funds are reestablished in the system through various transactions that look 'legitimate'. These transactions include purchasing of real estate land, luxury item or investments which appear clean on the face of it but at the same time integrate the illicit funds into the economy

Compensation:

Money Mules may receive a percentage of the laundered funds as payment for their role in the operation, although they often bear significant legal and financial risks, including criminal prosecution and financial penalties.



Risks associated with Money Mules

Money mule operations poses severe consequences to financial institutions, both legally and financially due to increased regulatory focus in this space. Here are few potential risks that financial institutions may face in today's world with the evolving threat of money mule:

Money laundering

Money Mules often receive funds for crimes such as phishing or drug trafficking and later transfer money to other accounts or organisations as instructed. By doing so, they knowingly or unknowingly facilitate money laundering activity.

Cyber

Money Mules, recruited through online platforms or social engineering tactics may be tricked into providing their personal information, such as bank account details to fraudsters. Cyber criminals may use malware/hacking techniques to compromise the mule's devices and steal sensitive information.

Compliance

Banks are subject to stringent regulations aimed at preventing AML and CFT risks. Engaging in transactions involving Money Mules may expose banks to compliance violations, regulatory sanctions, and legal penalties. Failure to adequately detect and report suspicious transactions can result in fines, reputational damage, and loss of license to operate.

Legal

Banks may face legal liabilities arising from their involvement in money muling activities. This includes potential lawsuits from customers affected by fraudulent transactions, as well as legal action by regulatory authorities for non-compliance with anti-money laundering regulations.

Financial

Financial risk is faced by banks while processing transactions potentially linked with Money Mules like regulatory fines or penalties and losses due to fraud. Further, banks may incur costs related to investigating suspicious mule activities and addressing any resulting legal or regulatory issues.

Reputational

Banks' reputations can be severely impacted by their association with money muling activities. Being implicated in facilitating illicit financial transactions can erode customer trust, leading to customer attrition, negative media coverage, and damage to brand reputation.

Operational

Money muling activities can introduce operational vulnerabilities and inefficiencies within banks' systems and processes. Ineffective measures may result in lack of detection of suspicious transactions, leading to operational disruptions, financial losses, and regulatory scrutiny.

Strategic

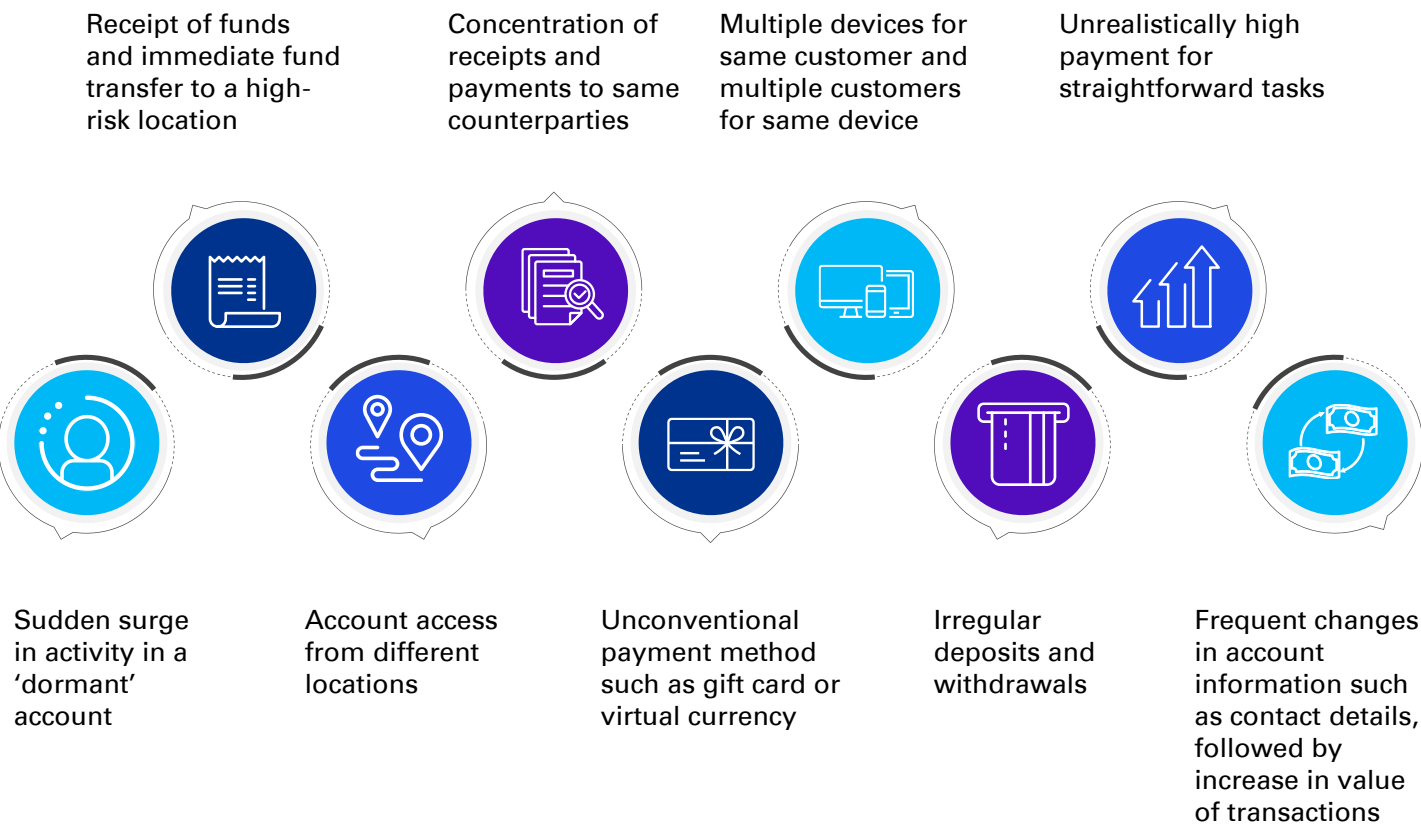
Failure to effectively address the risks associated with money muling can undermine banks' strategic initiatives, such as expansion into new markets, mergers and acquisitions, and digital transformation efforts affecting their long-term business objectives and growth prospects.



Is your institution infested with Money Mules?

Money mule operations poses severe consequences to financial institutions, both legally and financially due to increased regulatory focus in this space. Here are few potential risks that financial institutions may face in today's world with the evolving threat of money mule:

Indicative mule account transactional patterns:





What can FIs do to tackle money mule risks?

Money Mules complicate the process of detecting financial crimes thereby creating a significant AML/CFT compliance challenge. Firms that fail to detect them face severe risk of penalties, fines, censures, and reputational damage. FIs must ensure a robust AML program and take appropriate remedial actions to combat mules. Below are few actions FI may take to mitigate money mule risks¹¹:

Robust systems and controls

Strengthen existing AML and customer onboarding system to identify suspicious behaviour related to money mule typologies, including implementing a robust Customer Due Diligence (CDD) and Transaction Monitoring (TM) controls.

Investment in technology

Invest in AI/ML driven mule detection models along with other innovative solutions such as device intelligence & profiling, behavioural biometrics, and geolocation.

Threat based risk assessments

Threat-based periodic review of key systems and controls to assess its efficacy in detecting emerging risks like Money Mules. It is critical to identify and prioritise threats, measure inherent risks, perform control effectiveness review, and arrive at a residual risk with an action plan to mitigate the residual risks.

Staff training and customer awareness

Create a robust training and awareness programs for staffs and clients. Having a dedicated program on fraud and financial crime helps in keeping abreast with latest risk typologies such as Money Mules.

Effective reporting mechanism

Report suspicious or fraudulent transactions with regulators in the form of filing Suspicious Activity Reports (SARs). This is critical to break the mule network and helps enforcement agencies investigate the crimes further, identify the root causes and prosecute the perpetrators.

Increased focus in response and containment

Invest in building a strong investigative team with advanced analytical capabilities. This will ensure a swift event response and assist in having a containment measure in place, reducing the overall fraud impact on clients.

Market Intelligence to capture evolving risk themes

Foster an open communication channel for gathering credible intelligence from the market through information exchange with regulatory authorities, banks, and enforcement agencies. This may lead to an effective defense against emerging financial crime risks such as Money Mules.



The fight against Money Mules requires a unified, enterprise-wide approach that spans operations, technology, compliance, and corporate culture. It is imperative to drive institutional change by making Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) a C-suite priority.

**- Suveer Khanna,
Partner & Head,
Forensic
Investigation,
KPMG in India**



11. Opportunities and challenges of new technologies for AML/CFT, FATF

Acknowledgement

KPMG in India would like to thank the following for their contribution:

- Arnab Basak
- Dixita Bhalawat
- Samruddhi Shah
- Ashaar Sakaria
- Khushi Kansara



KPMG in India contacts:

Manoj Kumar Vijai

Office Managing Partner -
Mumbai & Head Risk Advisory

T: +91 98926 00654

E: mkumar@kpmg.com

Rajosik Banerjee

Head - FRM & Deputy Head - RA

T: + 91 98203 03556

E: rajosik@kpmg.com

Jagvinder S. Brar

Partner and Head

Forensic Services and F-Tech

T: +91 97169 09339

E: jsbrar@kpmg.com

Suveer Khanna

Partner and Head
Forensic Investigations

T: +91 96196 32131

E: skhanna@kpmg.com

Anoop Sharma

Director
Forensic Services

T: +91 98334 83595

E: anoopsharma@kpmg.com



Access our latest insights
on KPMG Insights Edge

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is meant for e-communication only. (011_BRO0524_KK)