FICCI 100
100 YEARS OF BUILDING TOMORROW

KHAITAN & CO
ADVOCATES SINCE 1911

Fraud in the Digital Age

Legal, Compliance and Enforcement Challenges

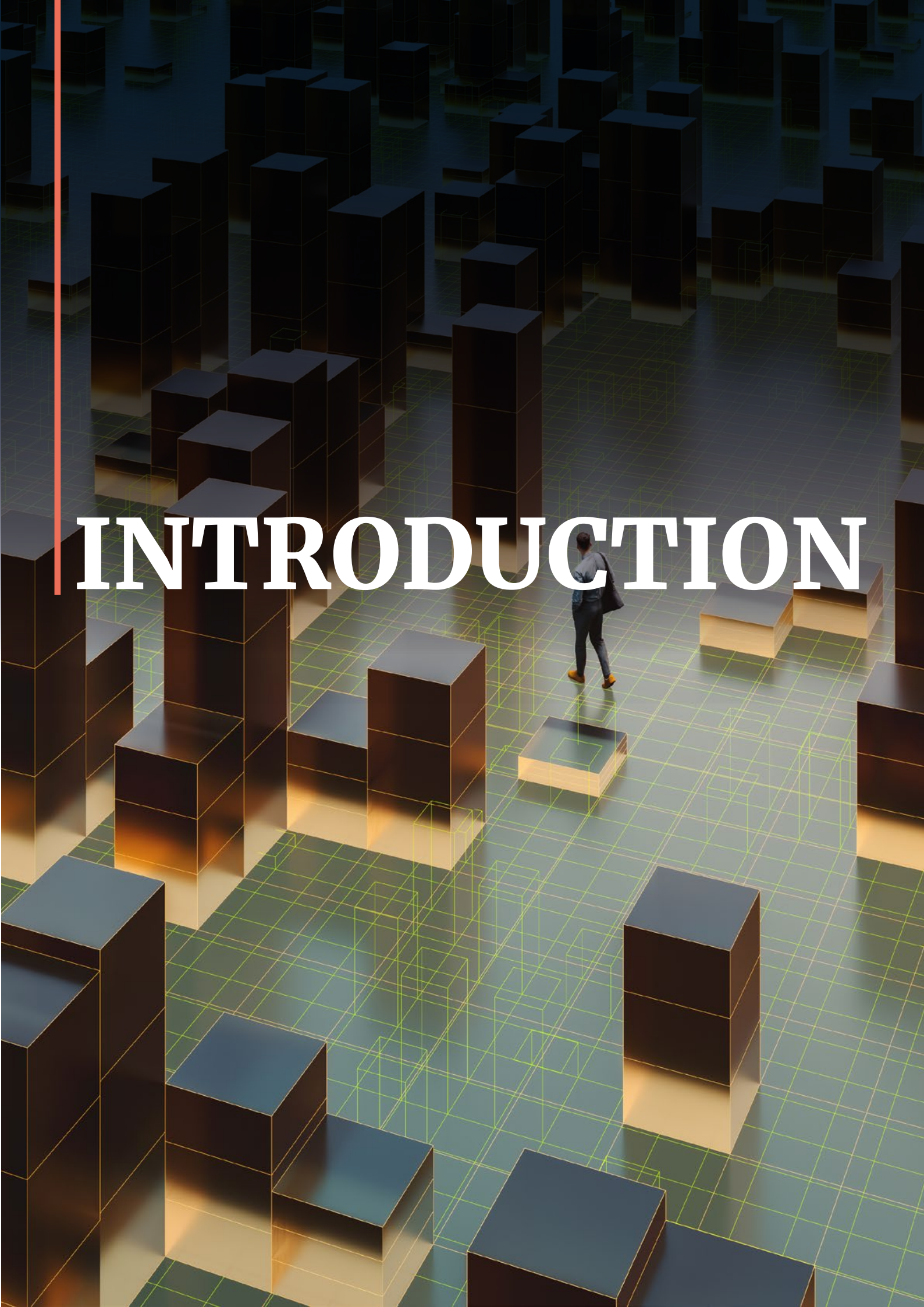
FOREWORD

As technology continues to transform the way institutions, businesses, and individuals operate, forensic investigations have become critical to ensuring legal compliance, regulatory oversight, and institutional accountability. The growing reliance on digital technologies, data-driven systems, and cross-border digital ecosystems has introduced complex challenges relating to electronic evidence, cyber crime, privacy, financial misconduct, and enforcement.

Addressing these challenges requires robust legal and regulatory frameworks, strengthened forensic capabilities, and closer collaboration among policymakers, regulators, enforcement agencies, industry, and legal professionals.

FICCI, in collaboration with Khaitan & Co, is pleased to present this Knowledge Paper, which examines the evolving legal, regulatory, and compliance dimensions of forensic investigations in India. We hope this publication serves as a valuable resource for stakeholders working towards a more resilient, transparent, and future-ready investigative and enforcement ecosystem.

Jyoti Vij
Director General
FICCI



INTRODUCTION

Over the past decade, digital payments in India have expanded at an unprecedented pace, reflecting a structural shift in the manner in which individuals and businesses conduct financial transactions. Digital transaction volumes have increased 38-fold, while transaction values have more than tripled. The Compound Annual Growth Rate (CAGR) of digital payments over this period stands at approximately 53% and 13% in volume and value terms respectively.

India's rapid economic growth, the expansion of digital financial services, and the growing sophistication of organised crime have together created a fraud landscape that is more complex and damaging than ever before.

The scale of financial fraud is already significant. According to the Reserve Bank of India's (RBI) Annual Report 2024-25, bank frauds involving more than INR 36,014 crore were reported during the financial year 2024-25, marking an almost threefold increase over the financial year 2023-24 in terms of the amount involved. The report further noted that digital payments and internet-based fraud accounted for the highest number of reported cases, while cyber-enabled fraud emerged as the fastest-growing category of financial fraud.

Beyond the figures, the nature of fraud itself has changed. Modern schemes are often built on digital infrastructure and designed to move faster than traditional enforcement systems can respond. Perpetrators are now taking advantage of digital payments, cloud platforms, social media, and artificial intelligence to run operations that can span multiple countries, mix real and virtual assets, and evolve quickly to avoid detection. This includes everything from complex trade-based money laundering to shell companies set up in offshore jurisdictions to move illicit funds.

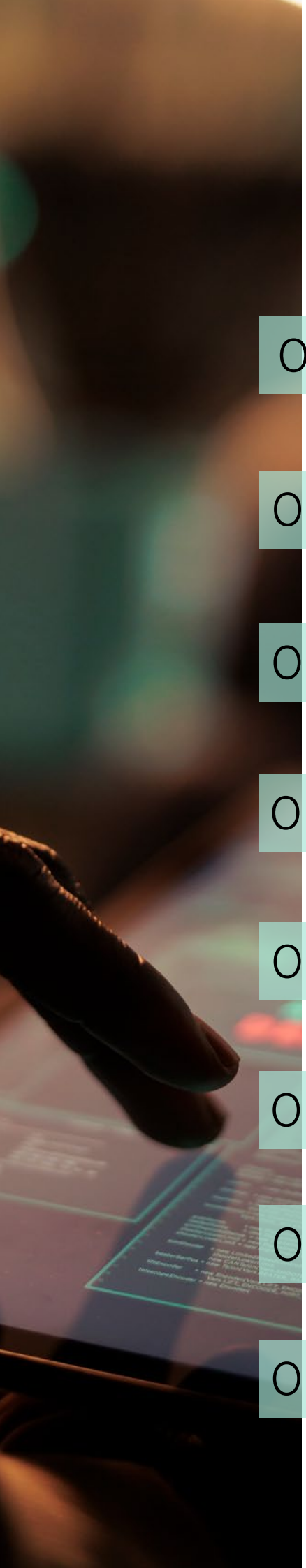
India's legal and regulatory architecture was largely designed for a slower, paper-based financial ecosystem. Today, investigative agencies, regulators, and courts are increasingly being required to address fraud typologies driven by artificial intelligence, cryptocurrency transactions, deepfakes, algorithmic trading, and cross-border digital infrastructure.

Several foundational statutes, including the Bharatiya Nyaya Sanhita, 2023 (BNS), the Companies Act, 2013 (Companies Act), the Prevention of Money Laundering Act, 2002 (PMLA), and theInformation Technology Act, 2000 (IT Act), continue to provide the principal enforcement framework. However, these statutes were not originally conceived for technology-enabled financial crime operating at digital speed and across multiple jurisdictions.

The resulting enforcement challenges are increasingly visible in practice. Fraud investigations today involve large-scale digital evidence, encrypted communications, offshore fund flows, cloud-based data storage, and rapidly evolving methods of concealment. Consequently, enforcement agencies and courts are often required to adapt traditional legal principles to apply to investigative realities that are significantly more complex than those contemplated when many existing laws were enacted.

Manavendra Mishra
Partner
Dispute Resolution
Khaitan & Co

Amey Mirajkar
Partner
Dispute Resolution
Khaitan & Co



Contents

01

Legal Framework Governing Fraud in India

Overview of the Key Legislation and Judicial Interpretation of Fraud in India

COMPANIES ACT

Section 447 of the Companies Act provides the principal statutory framework governing corporate fraud in India. The provision adopts an expansive definition of "fraud", covering acts, omissions, concealment of facts, and abuse of position committed with intent to deceive, obtain undue advantage, or injure the interests of the company, its shareholders, creditors, or any other person. The provision also prescribes stringent criminal consequences, including imprisonment and substantial monetary penalties, particularly in cases involving public interest.

The statutory framework governing auditors also plays an important role in fraud detection and reporting. The Guidance Note on Reporting of Fraud and SA 240 issued by the Institute of Chartered Accountants of India (ICAI) recognise that fraud may extend beyond conventional financial misstatements and may involve broader misconduct affecting the interests of companies, shareholders, and creditors. At the same time, these standards acknowledge the practical limitations faced by auditors in detecting sophisticated fraud schemes, particularly where the financial impact is not fully reflected in the books of account.

Consequently, the auditor's role is primarily directed towards identifying material misstatements, misappropriation of assets, and other indicators of fraud during the audit process.

Relevant extracts from SA240 for reporting standards for fraud are provided herein below:

> "3. Although fraud is a broad legal concept, for the purposes of the SAs, the auditor is concerned with fraud that causes a material misstatement in the financial statements. Two types of intentional misstatements are relevant to the auditor misstatements resulting from fraudulent financial reporting and misstatements resulting from misappropriation of assets. Although the auditor may suspect or, in rare cases, identify the occurrence of fraud, the auditor does not make legal determinations of whether fraud has actually occurred.:
>
> 11. For purposes of the SAs, the following terms have the meanings attributed below:
>
> (a) Fraud - An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage."

Further, relevant extracts of the Guidance Note are provided herein below:

> "...
> 29. Section 143(9) read with Section 143(10), requires the auditor to comply with the SAs issued by ICAI. Further, Section 143(2) requires the auditor to make out his report after taking into account, inter alia, the auditing standards. Accordingly, the term "in the course of performance of his duties as an auditor" may be understood to mean in the course of performing an audit in accordance with the SAs.
>
> 31. The definition of fraud as per SA 240 and the explanation of fraud as per Section 447 of the 2013 Act are similar, except that under Section 447, fraud includes 'acts with an intent to injure the interests of the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.'
>
> However, an auditor may not be able to detect acts that have intent to injure the interests of the company or cause wrongful gain or wrongful loss, unless the financial effects of such acts are reflected in the books of account/financial statements of the company....
>
> 32. Therefore, for the purpose of Section 143(12) the auditor would need to consider the requirements of the SAs, insofar as they relate to the risk of fraud, including the definition of fraud as stated in SA 240, in planning and performing his audit procedures in an audit of financial statements to address the risk of material misstatement due to fraud."

Furthermore, the Guidance Note on the Companies (Auditor's Report) Order, 2020 (as amended in 2022) (Guidance on CARO) provides that the definition of fraud under the SA 240 is similar to the one provided under the explanation to Section 447 of the Companies Act. However, it also caveats the reporting obligation by stating that an auditor may not always be able to defect acts that have the intent to injure the interest of the company or cause wrongful gain,

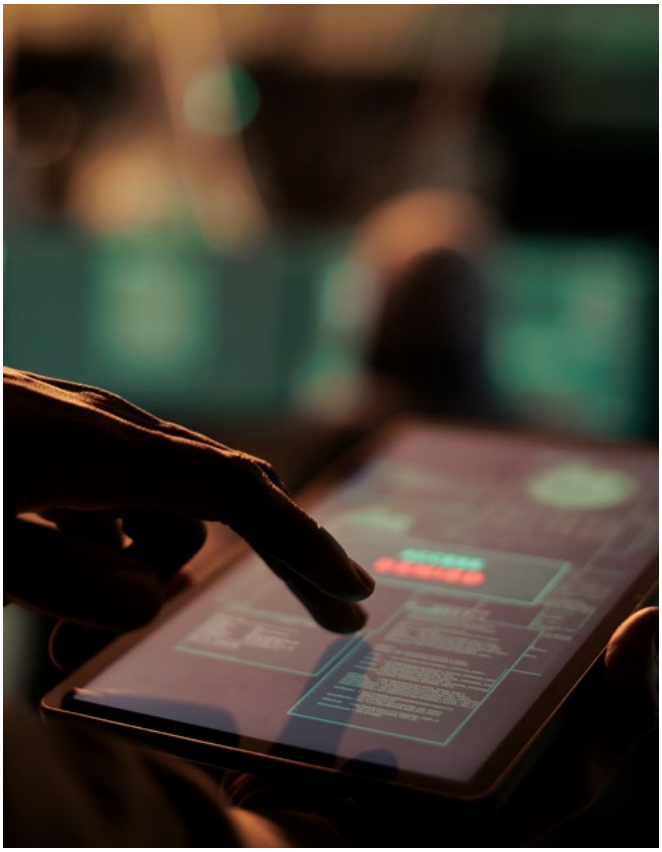
unless the financial effect of such acts is reflected in the books of account. The relevant extract of the Guidance on CARO is provided herein below:

> "70 (b)…
> The term 'fraud' as defined in explanation to section 447 of the Act in relation to affairs of a company or any body corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss. The term "fraud" is defined in SA 240 as "An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage".
>
> The definition of fraud as per SA 240 and the explanation of fraud as per section 447 of the Act are similar, except that under section 447 of the Act, fraud includes 'acts with an intent to injure the interests of the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.' However, an auditor may not be able to detect acts that have intent to injure the interests of the company or cause wrongful gain or wrongful loss, unless the financial effects of such acts are reflected in the books of account/financial statements of the company….."

SA 240 elaborates on the characteristics of fraud as follows:

Misstatements in the financial statements can arise from either fraud or error. The distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional.

Although fraud is a broad legal concept, the auditor is concerned with fraud that causes a material misstatement in the financial statements. Two types of intentional misstatements are relevant to the auditor - misstatements resulting from fraudulent financial reporting and misstatements resulting from misappropriation of assets.



The auditing framework under SA 240 therefore treats fraud principally as an intentional act involving deception resulting in material misstatement of financial statements or misappropriation of assets. At the same time, the guidance issued by ICAI recognises the practical limitations faced by auditors in identifying fraudulent conduct where the financial impact is not adequately reflected in the books of account. Consequently, the fraud assessment framework under Indian company law operates through a combination of statutory interpretation, audit standards, and evidence-based thresholds requiring objective material before allegations of fraud can be sustained.

BHARATIYA NYAYA SANHITA, 2023

The BNS is the revamped criminal code of India that replaced the erstwhile Indian Penal Code 1860 (IPC) and came into effect on 1 July 2024.

Although the BNS does not provide for a comprehensive definition of "fraud", there are provisions such as Cheating, Criminal Breach of Trust, Forgery, Falsification of Accounts, and other offence relating to documents and property marks that deal with aspects relating to fraud.

This gap of "fraud" not being defined within the BNS means that Indian prosecutors must fit modern fraudulent conduct, such as algorithmic manipulation or AI-generated misrepresentation, into categories designed for physical-world deception. While, the BNS does not explicitly define 'fraud', the statute under Section 2(9) defines 'fraudulently' to mean "doing anything with the intention to defraud but not otherwise".

PMLA

In India, the PMLA constitutes the principal legislation enacted to address the offence of money laundering. Offences under the PMLA are triggered upon the existence of a scheduled offence as specified in the Schedule to the PMLA. Although money laundering is treated as a distinct offence under the PMLA, it necessarily arises from the existence of "proceeds of crime" generated, possessed, concealed, used, projected, or claimed as untainted property from a scheduled offence investigated by another law enforcement agency.

A scheduled offence refers to an underlying offence that gives rise to the initiation of proceedings for money laundering under the PMLA. The Schedule to the PMLA enumerates such offences which, if committed, may result in the generation of proceeds of crime and thereby trigger the jurisdiction of the ED. Therefore, notably the investigation under the PMLA is ordinarily triggered only upon the existence of a predicate/ scheduled offence being investigated by a competent law enforcement agency through registration of a first information report (FIR), complaint, chargesheet, or other cognisable enforcement process.

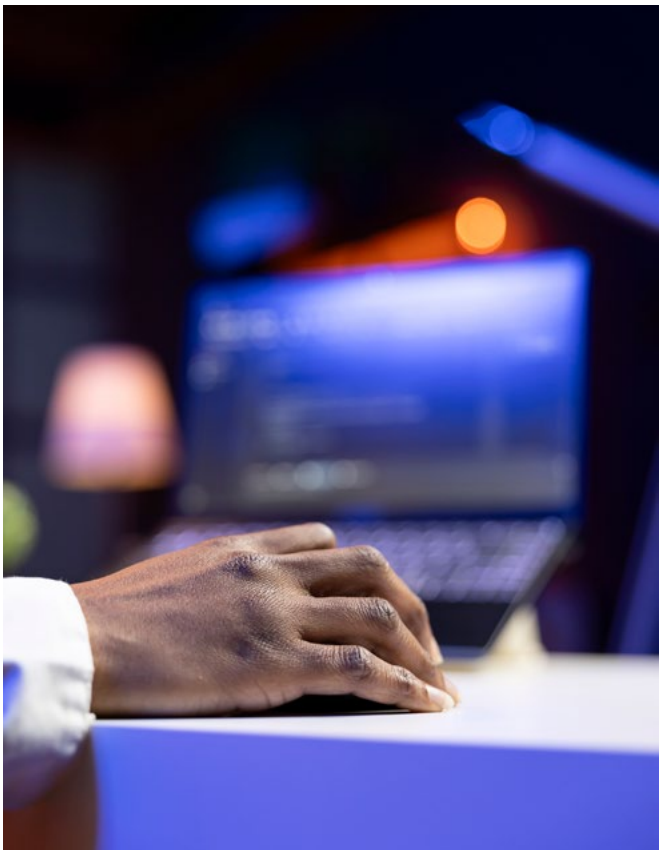
With respect to fraud, Section 447 of the Companies Act, and certain offences relating to cheating and forgery form a part of the schedule to the PMLA, and therefore, any investigation initiated qua such provisions might give rise to an investigation being initiated under the PMLA. As a result, major fraud investigations in India increasingly operate through a dual-enforcement structure, where the predicate offence is investigated by one agen-

cy while the consequential proceeds-of-crime investigation is simultaneously pursued by the Directorate of Enforcement (ED) under the PMLA.

IT ACT

The IT Act constitutes the principal statutory framework governing cyber-enabled offences and digital fraud in India. It establishes both civil and criminal liability for unlawful activities conducted through computer systems, electronic networks, and digital communication platforms. Among its key provisions, Section 66C criminalises identity theft, including the dishonest or fraudulent use of another person's electronic signature, password, or unique identification credentials, and Section 66D addresses cheating by personation through computer resources, thereby covering offences such as phishing, impersonation scams, fraudulent online representations, and other deceptive digital practices used to induce victims into parting with money or sensitive information.

The IT Act further provides remedies for unauthorised access, data breaches, and cyber intrusions. Section 43 imposes civil liability for acts such as unauthorised access to computer systems, downloading or copying data without permission, introducing malware or viruses, disrupting network operations, or causing damage to digital infrastructure. Where such acts are committed dishonestly or fraudulently, Section 66 elevates the conduct into a criminal offence punishable with imprisonment and fines. Together, these provisions form the legal basis for prosecuting hacking, data theft, ransomware incidents, and other forms of cyber intrusion.



STANDARD OF PROOF IN FRAUD AND DIGITAL FRAUD

Since fraud under Section 447 of the Companies Act constitutes a criminal offence, the applicable standard of proof is the same as that in other criminal proceedings, namely, proof beyond reasonable doubt. The Supreme Court and the Bombay High Court have consistently held that allegations of fraud must be established to this stringent standard.[1] Mere suspicion or conjecture is insufficient; rather, the finding of fraud must be supported by cogent material and credible evidence demonstrating the commission of the offence.

[1] *Kisan Sahakari Chini Mills Ltd. v. Richardson and Cruddas (1972) Ltd., (1999) 96 Comp Cas 776; Chemicals Pvt. Ltd. v. Chemicals Pvt. Ltd. with Aviat Chemicals Pvt. Ltd., 1999 SCC OnLine Bom 243*

The Supreme Court in Union of India v. Chaturbhai M. Patel & Co., (1976) 1 SCC 747 has held that:

> "It is well settled that fraud like any other charge of a criminal offence whether made in civil or criminal proceedings, must be established beyond reasonable doubt: per Lord Atkin in A.L.N. Narayanan Chettyar v. Official Assignee, High Court, Rangoon however suspicious may be the circumstances, however strange the coincidences, and however grave the doubts, suspicion alone can never take the place of proof. In our normal life we are sometimes faced with unexplainable phenomenon and strange coincidences, for as it is said, truth is stronger than fiction. In these circumstances, therefore, after going through the judgment of the high court we are satisfied that the appellant has not been able to make out a case of fraud as found by the high court. As such the high court was fully justified in negating the plea of fraud and in decreeing the suit of the plaintiff."

The Supreme Court in an order dated 01 December 2025 in the case of In Re: Victims Of Digital Arrest Related to Forged Documents, Suo Moto W.P. (Crl.) 3/2025 divided online scams/ frauds into three categories and while highlighting the gravity of these cases, directed the Central Bureau of Investigation to be the primary agency to investigate these cases.

Digital Arrest Scams

> "4. …
> This is a category of cybercrimes where victims are led to believe that their hard-earned money is owed to a government authority, and as a result, they are subjected to coercive acts of extortion.

Investment Scams

> These involve situations where victims are induced to deposit large sums under the guise of lucrative investment schemes, only to be subsequently defrauded. Fraudsters routinely invent new terms to deceive their targets, and in some cases, the funds have been taken under the pretext of 'advance tax'.

Part-Time Job Scams

> In these scams, victims are initially ttracted with small, free tasks—for instance, posting positive reviews or watching YouTube videos—and later, they are persuaded to deposit large sums of money by claiming it is for 'premium tasks.
>
> There can indeed be no manner of doubt that every type of cybercrime resulting in victim deception, especially involving senior citizens, whether categorised into three groups or otherwise, requires specialised investigation. However, digital arrest scams clearly demand the urgent attention of the country's leading investigative agencies. Accordingly, we direct that the Central Bureau of Investigation (CBI) shall be the primary agency to investigate cases reporting digital arrest scams."

02

Regulatory and Enforcement Architecture

India's anti-fraud enforcement ecosystem is intentionally decentralised and involves multiple specialised agencies exercising overlapping jurisdiction across corporate fraud, cybercrime, securities violations, corruption, and money laundering. While this structure enables sector-specific expertise, it also creates coordination challenges, procedural overlap, and fragmented investigative processes in complex fraud matters involving multiple statutes and jurisdictions.

Principal Enforcement Agencies

JURISDICTIONAL POLICE AND THEIR RESPECTIVE CYBERCRIME CELLS

The jurisdictional state police have the power to initiate a preliminary enquiry and thereto has a power to take cognisance of any fraudulent activity should a cognisable offence be identified. Once a cognisable offence is identified, the jurisdictional police must register an FIR under Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS).

Once the FIR is registered, the jurisdictional police conducts an investigation into the alleged offence and accordingly provide their investigation report/chargesheet before the respective court of law under Section 193 of the BNSS.

The cybercrime cells within the respective jurisdictional police station also deal with offence of cyber fraud. The Indian Cyber Crime Coordination Centre (I4C), established under the Ministry of Home Affairs, provides a national coordination mechanism, operates the National Cyber Crime Reporting Portal (cybercrime.gov.in), and runs the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) for rapid freezing of fraudulently transferred funds with respect to cyber fraud.

CENTRAL BUREAU OF INVESTIGATION (CBI)

CBI is a premier investigating police agency in India. It is established under and derives its investigative powers from the Delhi Special Police Establishment Act, 1946.

The CBI retains jurisdiction over fraud cases involving central government employees, public sector undertakings, and cases referred to it by the Supreme Court or High Courts. Its Special Crime Branch and Banking Securities & Fraud Cell handle major bank fraud matters.

SERIOUS FRAUD INVESTIGATION OFFICE (SFIO)

The SFIO was constituted under Sections 211 and 212 of the Companies Act to investigate serious instances of corporate fraud, including offences under Section 447 of the Companies Act. Operating under the Ministry of Corporate Affairs, the SFIO is a specialised, multidisciplinary agency comprising professionals from fields such as forensic auditing, law, taxation, accountancy, information technology, etc.

The SFIO exercises exclusive jurisdiction in matters assigned to it and is vested with the powers of an inspector under Section 217 of the Companies Act, including the power to arrest. It also possesses powers akin to a civil court under the Code of Civil Procedure, 1908 (CPC) for investigative purposes, such as directing the production of books of account and other documents, summoning and examining individuals on oath, and inspecting company records at any place, with statements recorded during such examinations being admissible as evidence. Upon completion of an investigation, the SFIO submits its report to the Central Government, which may thereafter direct the initiation of prosecution against the company and its officers or employees.

A critical question that arises is who has the authority to direct SFIO to conduct investigations. Under Section 212 of the Companies Act, 2013, the Central Government may order an SFIO investigation on its own or upon a report by the Registrar of Companies or an Inspector.

This legal framework was recently considered by the Supreme Court in Yerram Vijay Kumar v. State of Telangana, 2026 SCC OnLine SC 44, where the Court clarified that offences relating to fraud under the Companies Act cannot be initiated through private criminal complaints. The decision is significant because it reinforces the specialised statutory framework governing SFIO prosecutions and limits the use of parallel private criminal proceedings in matters involving serious corporate fraud under the Companies Act.

DIRECTORATE OF ENFORCEMENT (ED)

The ED is a specialised financial intelligence and law enforcement agency functioning under the Department of Revenue within the Ministry of Finance. Its primary mandate includes the investigation of offences relating to money laundering under the PMLA and violation of the Foreign Exchange Management Act, 1999 (FEMA).

The ED has also been actively handling cyber fraud-related cases. Till 28.02.2026, the ED had taken up around 257 cybercrime cases for investigation, leading to the identification of Proceeds of Crime worth INR 35,925.58 crore.[2]

NATIONAL FINANCIAL REPORTING AUTHORITY (NFRA)

NFRA is a critical pillar of India's fraud enforcement architecture. Established under Section 132 of the Companies Act, 2013, NFRA has the mandate to oversee the quality of auditing and accounting standards for certain classes of companies, and to investigate professional misconduct by statutory auditors of such companies. Under Section 132(2) of the Companies Act, 2013, the NFRA is responsible for recommending accounting and auditing standards for approval by the Central Government, ensuring compliance with these standards, and overseeing the quality of services provided by professionals involved in maintaining such compliance. It also works towards improving the overall quality of accounting and auditing practices and carries out any additional functions related to these responsibilities.

Further, Rule 4(1) of the National Financial Reporting Authority Rules, 2018 (NFRA Rules), states that the NFRA is entrusted with protecting public interest, as well as the interests of investors, creditors, and other stakeholders, by promoting high standards in accounting and auditing and by effectively supervising the accounting and auditing functions of companies, corporate bodies, and auditors covered under the Rules.

Most recently, NFRA issued a circular in January 2026 prescribing enhanced requirements for communication between statutory auditors and those charged with governance — i.e., management and the Board. This circular is designed to ensure that

[2] *Press Release dated 24 March 2026, Ministry of Home Affairs, Cybercrime proceeds linked to Money Laundering networks (available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244499&reg=3&lang=2)*

auditors more effectively identify and communicate deficiencies in internal controls and fraud risks during the audit process, thereby strengthening fraud detection at the audit stage.

In practice, NFRA's investigative powers are constrained by several limitations. Its orders are not yet uniformly available in the public domain, which limits their value as a deterrent and as guidance for the auditing profession. The Central Information Commission has directed NFRA to make its orders publicly available and compliance with this direction would improve transparency significantly.[3]

NFRA has also clarified that the reporting obligation cast upon statutory auditors under Section 143(12) of the Companies Act is mandatory and independent of whether the fraud was first detected by another person or agency. Consequently, even where a fraud has already been identified internally or by another regulator, the statutory auditor remains independently obligated to assess and report the matter in accordance with the Companies Act framework.

There are also pending legislative proposals to enhance NFRA's powers under the Companies Act. These proposals, if enacted, would expand NFRA's jurisdiction and enforcement capacity. However, the auditing profession has expressed concerns that expanded NFRA powers may create overlapping or conflicting regulatory obligations alongside ICAI's existing disciplinary framework. The paper recommends that any law reform in this area should clearly delineate the respective roles of NFRA and ICAI to avoid enforcement gaps or duplication.

SECTOR SPECIFIC REGULATORS

The Securities and Exchange Board of India (SEBI) has extensive quasi-judicial powers in the securities fraud domain, including search and seizure, disgorgement, debarment, and prosecution. The RBI also supervises financial institutions for fraud risk management under its master directions on frauds. The Insurance Regulatory and Development Authority (IRDAI) also plays an analogous role for insurance fraud.

In recent times, multiple sector specific regulators are signing Memorandum of Understandings (MoUs) to share multiple data points that would assist the law enforcement agencies to identify fraud and take necessary action.[4]

---

[3] *Neha Katana v. CPIO: National Financial Reporting Authority, 2026 SCC OnLine CIC 511*
[4] *Press Release dated 09 April 2026, Ministry of Home Affairs, Financial Intelligence Unit-India and Indian Cyber Crime Coordination Centre sign landmark MOU to combat cyber fraud and financial crimes (available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2250459&reg=1&lang=1)*

03

Key Legal Challenges in Fraud Investigation

Admissibility of Digital Evidence

Digital evidence encompassing emails, WhatsApp messages, transaction logs, server records, cloud data, and device extractions, now constitutes the evidentiary backbone of virtually every fraud investigation. Yet India's evidence law, the Bharatiya Sakshya Adhiniyam, 2023 (BSA), although enacted in 2023, was designed for a traditional, pre-digital world.

Section 63 of the BSA has been the principal source of evidentiary controversy. The provision requires that electronic records be accompanied by a certificate signed by a responsible official of the computer system from which the record is produced, attesting to specified conditions. The Supreme Court's evolving interpretation of this provision from Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 which made Section 65B certification mandatory, to Shafhi Mohammad v. State of HP, (2018) 2 SCC 801 which introduced relaxations, to Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 which reasserted the primacy of 65B certification has created persistent uncertainty for investigators and prosecutors.

The BSA has attempted to modernise the framework by introducing a broader definition of "electronic record" and streamlining certification requirements. However, the law on authentication of records extracted from third-party platforms (such as foreign cloud service providers), forensic copies of seized devices, and metadata remains unsettled.

Data Privacy v. Investigation Requirements

The Digital Personal Data Protection Act, 2023 (DPDPA) marks India's first full-scale attempt to build a structured data protection system. It does allow certain exemptions for law enforcement under Section 17, but the exact boundaries of these exceptions are still unclear. In particular, questions remain about how far data fiduciaries can comply voluntarily and whether investigation agencies can directly demand data without seeking court approval. These issues have not yet been fully interpreted by the courts.

Until clearer guidance emerges, investigators are operating in a grey area. They often need quick access to sensitive personal data such as bank transactions, communications, and location information while also having to navigate a developing privacy regime that is beginning to recognise stronger individual rights.

This tension is especially visible in financial investigations. Agencies like FIU-IND regularly access detailed banking data, and the ED uses powers under Section 50 of the PMLA to summon documents without the kind of warrant-based safeguards seen in many common law systems. However, since the Supreme Court's landmark judgment in K.S. Puttaswamy v. Union of India, 2017 (10) SCC 1, which recognized privacy as a fundamental right, these practices are increasingly open to constitutional scrutiny. The key question of how to balance investigative efficiency with privacy rights remains unsettled.

Cross Border Enforcement Challenges

Fraud in the digital era is rarely confined within borders. Offenders often set up companies in offshore jurisdictions, move money through complex banking networks, and run operations like call centres from countries where cooperation with Indian authorities is slow or limited. This makes investigations significantly more difficult and layered. Several structural challenges stand out:

India's Mutual Legal Assistance Treaty (MLAT) network is relatively limited compared to the scale of cross-border financial crime it needs to address. In practice, getting evidence from jurisdictions such as the UAE, Singapore, and various Caribbean offshore centres can take a very long time, sometimes stretching into years, especially when formal cooperation channels are involved.

India is also not a party to the Budapest Convention on Cybercrime, which is designed to simplify and speed up access to electronic evidence across borders. While accession has been discussed, concerns around data sovereignty have slowed progress.

Extradition frameworks are similarly uneven. India has treaties with several countries, but not all key jurisdictions are covered.

Cryptocurrency adds another layer of complexity. Transactions can be pseudonymous, funds can be moved through mixers or across multiple blockchains, and some exchanges operate in jurisdictions with

weaker know-your-customer standards. This makes tracing money flows more difficult for traditional financial intelligence systems.

Investigations are further complicated by encrypted communication platforms, data localisation restrictions, cloud-based evidence storage, and varying levels of cooperation from multinational technology intermediaries. These issues often delay evidence collection and create additional procedural complexity in cross-border fraud matters.

Procedural and Litigation Bottlenecks

India's criminal justice system faces significant structural challenges, including heavy caseloads and procedural delays that affect the pace of adjudication. Specialised courts established under the PMLA and designated CBI courts represent a meaningful step towards more efficient resolution of financial and corruption matters; however, these forums continue to operate under considerable pressure. Consequently, complex fraud cases — including those arising from banking irregularities in the early 2010s — frequently remain pending for extended periods, reflecting systemic constraints rather than any absence of institutional intent.[5]

Prolonged proceedings carry practical implications for the integrity of the trial process. Extended timelines can affect the reliability of witness recollection, create challenges in the preservation and authentication of documentary evidence, and provide scope for procedural delays. Addressing these challenges is essential to strengthening the overall effectiveness of prosecution and ensuring that enforcement mechanisms retain their intended deterrent value.

[5] *Over 7,000 CBI graft cases await trial in courts: https://www.thehindu.com/news/national/more-than-7000-graft-cases-probed-by-cbi-pending-trial-in-courts-379-for-over-20-years-central-vigilance-commission/article69995924.ece#google_vignette*

04

Corporate Liability and Governance

Board and Management Responsibilities

The Companies Act imposes specific duties on directors and Key Managerial Personnel (KMPs) that have direct relevance to fraud prevention and corporate governance. Section 166 requires directors to act in accordance with the articles, in good faith, in the best interests of the company and its stakeholders, and with due and reasonable care. Section 149(8) requires independent directors to satisfy themselves of the integrity of financial information, the adequacy of financial controls, and the robustness of risk management systems.

A key feature of the Companies Act is that it places responsibility not only on the company as an institution, but also on the individuals managing it. Under the concept of the "officer in default" in Section 2(60), liability can extend to managing directors, whole-time directors, company secretaries, and other senior officials responsible for the company's operations. In serious fraud cases, Section 447 even allows for imprisonment, making fraud prevention and compliance a matter of personal accountability for senior management rather than simply a corporate obligation.

The law also strengthens internal oversight mechanisms. Audit Committees constituted under Section 177 are required to assess the effectiveness of internal financial controls, review risk management systems, and establish

whistle-blower mechanisms so that concerns can be reported safely within the organisation.

At the judicial level, courts have tried to balance corporate autonomy with accountability. In Sanjay Dutt v. State of Haryana, 2025 SCC OnLine SC 32, the Supreme Court reaffirmed that directors cannot automatically be held liable for every act committed by a company. Consequently, investigations by agencies such as the SFIO have increasingly succeeded in "lifting the corporate veil" where directors were found to be actively involved in fraudulent schemes or exercising controlling influence over them.

Increasingly, fraud incidents are also being evaluated through the lens of governance and ESG (Environmental, Social, and Governance) compliance. Under the evolving SEBI LODR framework and Business Responsibility and Sustainability Reporting (BRSR) requirements, listed companies are expected to strengthen internal controls, whistleblower mechanisms, risk management systems, and ethical governance practices.

Consequently, fraud exposure today creates not only legal and financial consequences, but also significant reputational, governance, and investor-confidence risks for companies and their management.

Legal Implications of Fraud Incidents

When fraud occurs within or against a company, the consequences rarely remain limited to a single legal issue. Instead, they often trigger obligations and liabilities across several regulatory and legal frameworks at the same time.

For listed companies, securities laws require prompt disclosure of material frauds to stock exchanges under the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR). Failure to disclose such events can invite enforcement action from SEBI. Banks are also subject to reporting obligations under the RBI's Master Direction on Frauds, which requires frauds above certain thresholds to be reported within prescribed timelines. In addition, the PMLA imposes obligations to file Suspicious Transaction Reports (STRs) in cases involving potentially unlawful financial activity. A failure to comply with any of these reporting requirements can create separate regulatory exposure, apart from the fraud itself.

The risks are not confined to the company alone. Directors and KMPs may face personal criminal liability under Section 447 of the Companies Act, along with civil claims from shareholders and regulatory penalties such as disqualification or debarment from holding board positions. Additional complications can arise under the SEBI (Prohibition of Insider Trading) Regulations, 2015 if non-disclosure of fraud overlaps with trading in the company's securities.

Although many large Indian companies now maintain Directors and Officers liability insurance, these policies often exclude coverage in cases where the insured individuals themselves are accused of participating in the fraud rather than being victims of it. As a result, senior management can face significant personal and financial exposure when corporate fraud allegations emerge.

Internal Investigation and Compliance Frameworks

An effective internal investigation that is carried out quickly, independently, and with strong forensic support is increasingly seen as essential in responding to corporate fraud. Such investigations not only help organisations identify and address misconduct but can also influence how regulators and prosecutors respond to the case. Around the world, and increasingly in India as well, authorities tend to view companies more favourably when fraud is detected through strong internal controls and voluntarily reported along with the findings of a credible investigation.

At the same time, India's legal framework for internal investigations continues to develop, reflecting the country's evolving approach to corporate governance and enforcement. While jurisdictions such as the United States and the United Kingdom have established formal deferred prosecution agreement mechanisms — enabling companies to avoid prosecution in exchange for cooperation, remediation, and compliance reforms — India is at a different stage of this journey. Encouragingly, certain regulatory bodies have already introduced settlement mechanisms tailored to their respective domains, such as SEBI's settlement process under the SEBI (Settlement Proceedings) Regulations, 2018, and the Competition Commission of India's leniency programme for cartel cases.

A comprehensive framework specifically designed for resolving corporate fraud matters through negotiated settlements has yet to emerge, though this represents a recognised area for future development. The need for such a framework has been brought into sharper focus by recent enforcement actions, underscoring the value of providing clearer, more predictable outcomes for companies that cooperate proactively with regulators.

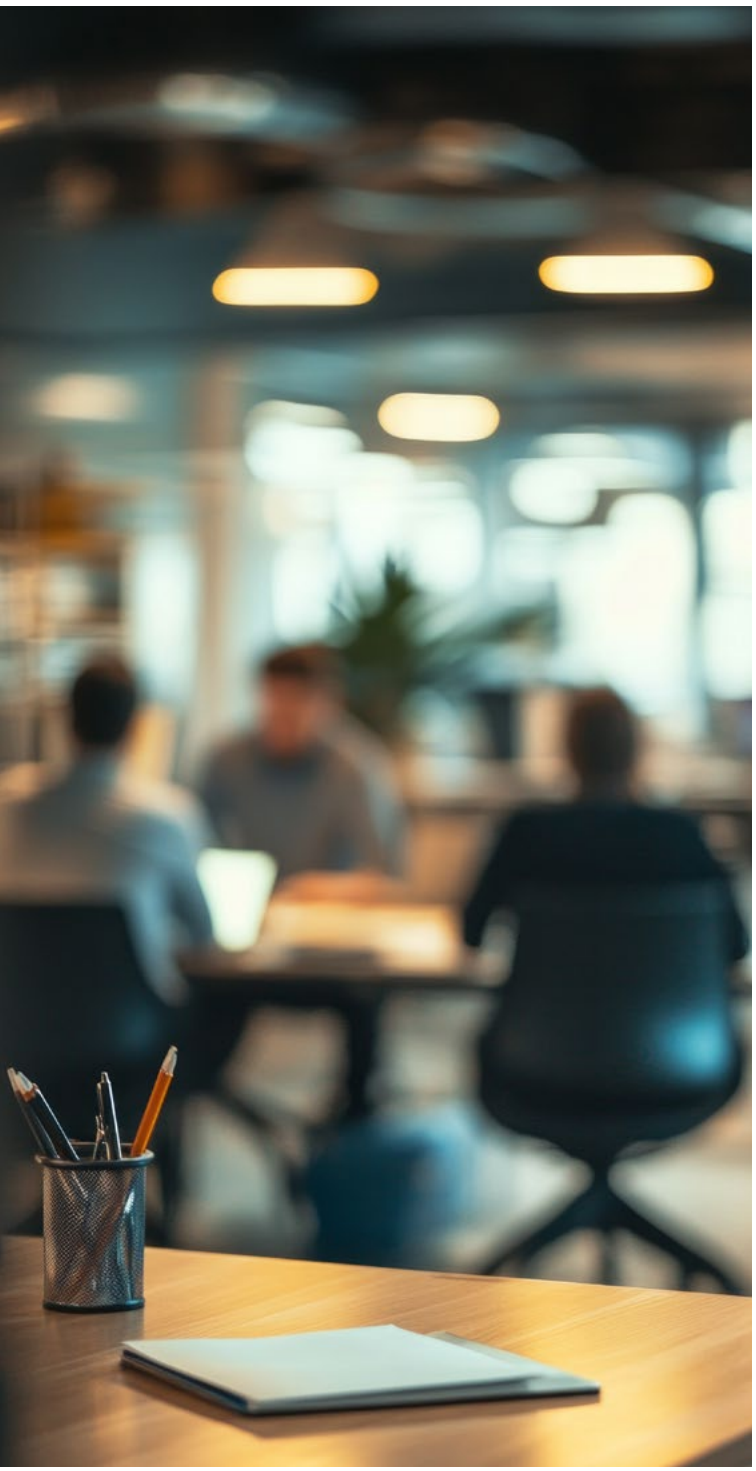
The Supreme Court's decision in Hyeoksoo v. Moon June Seok, 2025 SCC OnLine SC 759, is an important precedent illustrating how collusion between internal finance personnel and external professionals can undermine corporate financial controls. The case involved allegations that senior finance officials diverted company funds under the guise of GST payments and received unlawful kickbacks through intermediary entities. The judgment underscores the growing importance of forensic accounting, internal controls, and independent investigations in detecting sophisticated accounting and procurement fraud within corporate structures.

In practice, strong corporate compliance systems are becoming increasingly important. In the Indian context, effective fraud prevention frameworks should include regular fraud-focused risk assessments, strong Know Your Customer (KYC) and Know Your Business (KYB) procedures, independent whistle-blower channels backed by clear non-retaliation policies, and real-time transaction monitoring supported by data analytics.

Regular employee training on fraud risks and active oversight by the Audit Committee are also critical to ensuring that fraud prevention becomes part of an organisation's governance culture rather than merely a compliance formality.

05

Emerging Legal Issues



Organised Crime

An emerging and deeply concerning aspect of organised financial crime is the rise of "scam farms" across parts of South-East Asia, particularly in countries such as Cambodia, Myanmar, and Laos. These facilities are reportedly operated by transnational criminal networks that traffic individuals, including Indian nationals, and coerce them into carrying out large-scale online fraud schemes targeting victims across the world. The phenomenon has been documented by both the National Investigation Agency and the United Nations Office on Drugs and Crime.[6] In 2024, the Madurai Police arrested an individual allegedly involved in trafficking Indian nationals to cyber-scam compounds in Cambodia. These operations reflect a disturbing intersection of human trafficking, forced labour, and sophisticated financial fraud, underscoring the urgent need for coordinated international law enforcement and regulatory cooperation.

India's present legal framework remains imperfectly equipped to address fraud operations emerging from organised cyber-scam networks operating across Southeast Asia. Although Section 75 of the IT Act provides limited extraterritorial jurisdiction, enforcement remains difficult in practice where the underlying conduct is not effectively criminalised or prosecuted in the host

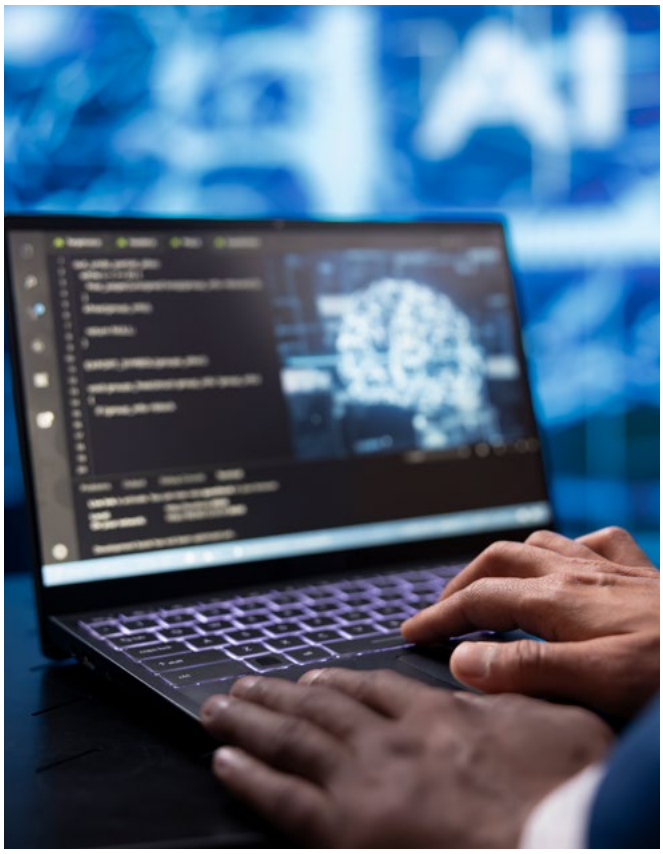
[6] *NIA Press Release dated 18 February 2026, NIA chargesheets 3 Accused in Myanmar-based Human Trafficking & Cyber Fraud Case; (available at: https://nia.gov.in/sites/default/files/Document/enc_1fb-8819c3bdbb5f3f9f675fcf3849768.pdf), UNODC, Crushing scam farms, Southeast Asia's 'criminal service providers' (available at: https://www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms--southeast-asias-criminal-service-providers.html)*

jurisdiction. While the expansion of the PMLA framework to cryptocurrency transactions represents a significant development, concerns continue regarding the pace of prosecutions, international evidence-sharing, and operational cooperation mechanisms. The present framework therefore highlights the need for stronger mutual legal assistance arrangements, enhanced cross-border cyber enforcement mechanisms, and more coordinated financial intelligence systems targeting transnational fraud networks.

AI-Led Frauds and Regulatory Gaps

Artificial intelligence has increasingly become both a powerful tool for innovation and a growing source of fraud-related risks. On one hand, AI is now being used to create highly convincing fake documents such as bank statements, invoices, incorporation certificates, and audit reports that would previously have required substantial technical expertise to forge. AI-driven chatbots are also being deployed in large-scale scams, including investment frauds. In financial markets, automated trading systems and algorithmic trading tools have enabled market manipulation to occur at speeds and volumes that are often difficult for traditional surveillance systems to detect.

The rapid growth of algorithmic and AI-driven trading has created major challenges for regulators across the world. SEBI's recent findings showed that algorithmic trading accounted for an overwhelming share of profits in India's futures and options market during FY24, contributing to 97% of profits earned by foreign portfolio investors and 96% of profits earned by proprietary traders.[7] High-frequency trading (HFT) presents a particularly difficult enforcement challenge because manipulative conduct can occur at machine speed and leave only narrow re-al-time detection windows for regulators. Such systems may also be misused for practices such as spoofing, where orders are rapidly placed and cancelled to create artificial impressions of market activity or liquidity. In response, SEBI has introduced measures aimed at improving transparency, including requirements for unique algorithm identification and tighter controls on open APIs. While these steps reflect a stronger regulatory approach, concerns remain about enforcement. Past cases, including the NSE dark fibre controversy, have shown that delays in regulatory action can weaken the effectiveness of even well-designed guidelines.



[7] *SEBI PR No. 22/ 2024 dated 23 September 2024; Updated SEBI Study Reveals 93% of Individual Traders Incurred Losses in Equity F&O between FY22 and FY24; Aggregate Losses Exceed 1.8 Lakh Crores Over Three Years (available at: https://www.sebi.gov.in/media-and-notifications/press-releases/sep-2024/updated-sebi-study-reveals-93-of-individual-traders-incurred-losses-in-equity-fando-between-fy22-and-fy24-aggregate-losses-exceed-1-8-lakh-crores-over-three-years_86906.html)*

Despite India's rapid adoption of AI and digital technologies, the country still does not have a dedicated and comprehensive law governing artificial intelligence. Instead, AI-related concerns are currently addressed through existing frameworks such as the DPDPA, intellectual property laws, and intermediary regulations under the IT Act. Although these laws provide some safeguards relating to data protection and platform accountability, they do not fully address issues such as algorithmic transparency, automated decision-making, deepfakes, ownership of AI-generated content, or accountability for AI systems.

India has taken gradual regulatory steps, particularly through amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Intermediary Guidelines), but the overall framework remains fragmented and largely reactive. Going forward, India is expected to adopt a more principles-based and gradual approach to AI regulation, with the aim of balancing innovation with safety, accountability, and alignment with evolving global standards.

Cryptocurrency-Related Challenges

Cryptocurrency has grown rapidly in India, driven by increasing digital adoption and a large tech-savvy population. At the same time, the rise of crypto has also brought a surge in frauds and scams, ranging from fake exchanges and ponzi schemes to phishing attacks and ransomware demands. Despite the growing scale of these risks, India still does not have a dedicated law specifically regulating cryptocurrencies or dealing exclusively with crypto-related crimes.

Although the Supreme Court's decision in Internet & Mobile Assn. of India v. RBI, (2020) 10 SCC 274 gave the sector some legitimacy by restoring banking access for crypto traders, the overall legal position remains uncertain. Because of this gap, enforcement agencies often rely on traditional laws under the Indian Penal Code and the Information Technology Act, 2000, even though these laws were never designed to deal with blockchain technology or digital assets.

Investigating cryptocurrency fraud is particularly difficult because transactions are often cross-border and can be carried out with a high degree of anonymity. Fraudsters may operate from other countries through decentralised platforms, making it difficult for Indian authorities to trace transactions, identify offenders, or recover stolen funds. Privacy-focused cryptocurrencies and advanced laundering techniques further complicate investigations. The lack of a clear regulatory framework has also left many investors vulnerable, as legitimate businesses and fraudulent schemes continue to operate side by side with limited oversight.

Following the cyberattack on a major crypto platform, criminal complaints under the BNS and the IT Act were made which lead to the registration of an FIR and the arrest of an individual allegedly involved in creating fake accounts on such crypto currency platform that used in the attack. Courts have treated such crypto-related frauds as serious economic offences with wider implications for public funds and the national economy, resulting in a stricter approach toward bail.[8] The Delhi High Court has also acknowledged the broader public-interest concerns associated with cryptocurrency transactions, particularly their anonymous and difficult-to-trace nature.[9]

[8] *Nimmagadda Prasad v. CBI, (2013) 7 SCC 466*
[9] *Umesh Verma v. State, 2025 SCC OnLine Del 8078*

In the aftermath of the breach, affected users approached the Supreme Court seeking measures such as a special investigation team, forensic audit, and freezing of crypto platform's assets. While the Supreme Court declined to entertain the plea on the ground that such matters fell within the domain of the executive and legislature, it permitted the petitioners to seek relief before the appropriate forum.[10]

Subsequently, proceedings were initiated before the Delhi High Court, which recognised the significant public investment involved in crypto platforms and sought responses from the Union of India, SEBI, RBI, and the crypto platform regarding the existing regulatory oversight framework and any proposed action against the platform.[11] The matter is currently pending final adjudication.

India has introduced some measures in recent years, such as taxing virtual digital assets and bringing crypto exchanges within the scope of the PMLA, which now requires KYC checks and transaction monitoring. The Financial Intelligence Unit - India (FIU-IND) is the designated authority for registering and regulating Virtual Digital Asset Service Providers (VDASP), including cryptocurrency exchanges, under the PMLA framework.

As of 2026, the FIU monitors nearly 50 VDASPs ensuring they comply with the PMLA. Only FIU-registered exchanges are legally permitted to operate in India, and those exchanges operating without registration are subject to enforcement action under the PMLA. Enforcement agencies have also started building expertise in blockchain forensics and crypto investigations. However, the overall regulatory approach is still evolving, and there is increasing recognition that India will need a more comprehensive legal framework, stronger enforcement capacity, and greater international cooperation to effectively tackle cryptocurrency fraud and protect investors

Deepfakes and Evidentiary Concerns

Deepfake technology, which uses artificial intelligence to create highly realistic but fabricated audio, video, or images, has emerged as a major challenge for both fraud prevention and the legal system. Fraudsters are increasingly using deepfakes in sophisticated scams, including impersonating company executives in financial transactions, creating fake KYC verification videos, and generating synthetic identities to bypass security systems. Because these recordings can appear extremely convincing, they make it much harder for individuals, businesses, and investigators to distinguish between genuine and manipulated content.

The problem becomes even more serious in legal proceedings. If a deepfake video or audio recording is presented as evidence, proving that it has been manipulated can be difficult, time-consuming, and expensive. Deepfake detection technologies continue to evolve and often require specialised forensic expertise, which may not always produce conclusive results. As courts increasingly rely upon electronic evidence in fraud prosecutions, the absence of clear evidentiary standards for authentication of AI-generated content creates a significant enforcement and evidentiary challenge.

---

[10] *Order dated 16 April 2025 in Hajarimal Bathra & Ors. Vs. Union of India & Ors., WP (Criminal) No. 161 of 2025,*
[11] *Order dated 15.01.2025 in Sudhir Verma & Anr. V. Union of India through the secretary to the Ministry of Finance & Ors., W.P.(C) 14969/2024 & CM APPL. 62785/2024.*

India currently does not have a specific law that directly deals with deepfakes. Some provisions under the Information Technology Act, such as Section 66E relating to privacy violations and Section 67A concerning sexually explicit content, provide limited protection in certain situations, but they were not designed to address deepfake-enabled financial or commercial fraud. Similarly, the Bharatiya Sakshya Adhiniyam, 2023, while recognising electronic records as evidence, does not specifically address AI-generated or synthetic media. As deepfake technology becomes more advanced and accessible, there is a growing need for dedicated legal provisions and clear technical standards for the forensic examination and authentication of AI-generated content.

Data Protection Considerations

The DPDPA introduces a new layer of responsibilities for organisations handling personal data, and these obligations have important implications for both fraud prevention and fraud investigations. By requiring companies to follow principles such as data minimisation, purpose limitation, and stronger security safeguards, the law encourages businesses to adopt privacy-focused systems that can also reduce the risk of data theft and related fraud.

At the same time, the DPDPA affects how investigations are carried out, particularly through provisions dealing with government exemptions under Section 17 and rules governing cross-border data transfers, both of which influence how Indian and foreign authorities may access personal data during investigations.

The situation is especially complex for financial institutions. Banks and other regulated entities are already required to collect, monitor, and analyse large volumes of customer data under RBI fraud management directions and SEBI surveillance requirements. These obligations are designed to detect suspicious activity and prevent financial crime.

However, the same institutions must now also comply with the privacy obligations introduced under the DPDPA. Balancing these competing responsibilities is not straightforward, and there is still limited clarity on how these frameworks will operate together in practice. As a result, stronger coordination between regulators, and possibly further legislative clarification, will likely be needed to resolve these overlaps and provide a more consistent compliance framework.

06

Case Law and Judicial Trends

The following are the landmark judgements that have shaped the legal framework in and around fraud:

State of U.P. v. Chhotey Lal, 2011 (2) SCC 550

The Court noted that offences such as crimes against the State, corruption, dowry death, domestic violence, sexual assault, financial fraud, and cybercrimes should all be fast-tracked and decided within a fixed timeframe. Although the case itself did not directly concern cyber fraud, the Court's remarks are important because they place cybercrime alongside some of the gravest categories of offences in the Indian legal system.

> *The observation is particularly significant in the context of modern digital fraud. By grouping cybercrimes with offences such as corruption and sexual violence, the Court acknowledged both the growing societal harm caused by such offences and the urgent need for stronger institutional responses. The judgment also highlighted systemic issues affecting criminal justice delivery, including inadequate investigative capacity, lack of technological infrastructure, frequent adjournments, and delays in evidence recording. In doing so, the Court recognised that effective enforcement against cyber fraud requires not only stronger laws, but also faster trials, better-trained investigators, and modern technological support within the justice system.*

In Re: Victims Of Digital Arrest Related to Forged Documents, Suo Moto W.P. (Crl.) 3/2025

The Court was hearing cases involving "digital arrest" scams, where fraudsters impersonated officials from agencies such as the CBI and Enforcement Directorate to coerce victims into transferring large amounts of money.

> *During the proceedings, the Court expressed serious concern over the scale of cyber fraud in India and the use of forged judicial documents, observing that such scams undermine public confidence in institutions. The widespread use of mule accounts opened across hundreds of bank branches, suggesting that the issue is not limited to isolated criminal acts but points to systemic weaknesses in banking oversight and monitoring. The case is pending before the Supreme Court as of mid-2026*

Hare Ram Singh v. Reserve Bank Of India & Ors., 2024 SCC OnLine Del 8039

The Delhi High Court in this case recognised that modern cyber frauds often involve sophisticated methods such as phishing, vishing, malware attacks, and SIM-related manipulation, where customers may become victims without actually sharing sensitive information like OTPs or PINs. In this case, the petitioner acted responsibly by promptly informing the bank and cybercrime authorities after discovering the unauthorised transactions. The Court observed that digital fraud today is frequently caused by weaknesses in banking security systems rather than customer negligence, and therefore innocent customers cannot automatically be held liable simply because fraudulent transactions occurred through their accounts.

> *The judgment also highlights the urgent need for stronger cybersecurity measures and faster response mechanisms within the banking system. Relying on RBI guidelines, the Court emphasised that banks must ensure secure digital payment systems, effective fraud detection, and timely action to prevent further loss once fraud is reported. By applying the "zero liability" principle, the Court reaffirmed that victims of cyber fraud should be protected where there is no evidence of negligence on their part. The ruling therefore strengthens consumer confidence in digital banking and sends a clear message that banks must adapt to evolving cyber threats while prioritising customer protection and accountability.*

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

The Constitution Bench decision in Arjun Panditrao Khotkar reaffirmed the mandatory nature of certification requirements for electronic evidence under Section 65B of the Indian Evidence Act (now reflected under the BSA framework). The judgment significantly impacted fraud and cybercrime prosecutions by emphasising that electronic records such as emails, chats, CCTV footage, and digital transaction logs must ordinarily be accompanied by valid certification establishing their authenticity and manner of production.

While the ruling has strengthened the reliability and integrity of digital evidence, it has also created practical challenges for investigators and prosecutors. In many fraud cases, electronic evidence comes from third-party platforms, cloud services, social media companies, or devices seized during investigation. Obtaining the required certification can become difficult when the relevant service provider is located outside India or when the person responsible for issuing the certificate is unavailable. As a result, even important digital evidence may face procedural hurdles despite being highly relevant to the case.

K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

The nine-judge constitutional bench decision recognising privacy as a fundamental right under Article 21 has begun to influence fraud-related adjudication, particularly in challenges to the surveillance and data access powers of enforcement agencies. While the decision has not yet directly curtailed the ED's powers, the proportionality test it introduced is increasingly invoked in High Court challenges to search and seizure operations, PMLA summonses, and data requisition orders.

The Concept of Digital Fraud has been Involving Through Various Judicial Interpretation which are as Follows:

Indian courts are increasingly being required to apply traditional legal principles to sophisticated forms of digital fraud and financial crime. As technology evolves faster than legislative reform, courts have frequently been compelled to interpret conventional concepts relating to deception, conspiracy, evidence, and financial misconduct within the context of online platforms, cyber-enabled fraud, digital assets, and algorithmic systems.

One noticeable trend is that courts have become more willing to accept digital communication records, such as emails, chats, call records, and metadata, as evidence of conspiracy or dishonest intent, provided the necessary procedural requirements are satisfied.[12] In particular, compliance with Section 63 of BSA, certification requirements and the support of expert testimony have become crucial in establishing the authenticity of electronic evidence.

In the area of securities fraud, regulatory enforcement has also evolved significantly. The decision of the Supreme Court in the case of SEBI v. Kishore R. Ajmera, 2016 (6) SCC 368, clarified that direct evidence of manipulation is not always necessary. Courts have accepted that trading patterns, timing correlations, communication records, and other surrounding circumstances can together establish manipulative intent in market abuse cases.

At the same time, Courts have shown increasing concern about the broad use of enforcement powers under the PMLA.[13] In particular, courts have started examining whether provisional attachment orders are being used proportionately, especially in situations where businesses are effectively paralysed or shut down before any final determination of guilt. This reflects a growing judicial effort to balance strong anti-fraud enforcement with procedural fairness and the protection of legitimate business activity.

[12] *Sharat Babu Digumarti v. Government of NCT of Delhi, (2012) 8 SCC 761*
[13] *Satendar Kumar Antil v Central Bureau of Investigation, (2021) 10 SCC 773*

07

Global Best Practices

United States of America (US)

The US is widely regarded as having one of the most advanced corporate fraud enforcement systems in the world. Its framework combines strong investigative powers, broad prosecutorial discretion, and well-developed mechanisms for international cooperation. Several aspects of the US approach offer useful lessons for India as it continues to strengthen its own anti-fraud and corporate compliance systems.

One of the most significant features of the US model is the use of Deferred Prosecution Agreements (DPAs) and Non-Prosecution Agreements (NPAs). Under these arrangements, companies accused of fraud can avoid a full criminal trial if they cooperate with authorities, pay financial penalties, improve internal compliance systems, and in some cases operate under the supervision of independent monitors. This system encourages companies to voluntarily disclose misconduct and work with investigators, while also reducing the long-term consequences that a criminal conviction can have on employees, shareholders, and business operations. India presently does not have a comparable institutional framework for negotiated corporate resolutions in fraud matters, thereby limiting incentives for early self-reporting, voluntary cooperation, and structured remediation.

Another important element is the strong enforcement of the Foreign Corrupt Practices Act (FCPA), which allows US authorities to pursue bribery and fraud cases even when conduct occurs outside the United States, provided there is some connection to the US financial system or markets. As a result, many Indian companies with US listings or business operations are already required to maintain high compliance standards to avoid FCPA liability.

The US has also developed sophisticated financial intelligence systems through agencies such as the Financial Crimes Enforcement Network (FinCEN). FinCEN maintains beneficial ownership databases, issues anti-money laundering regulations, and uses targeted monitoring tools in high-risk sectors such as real estate. These intelligence-driven approaches provide a useful example of how India's Financial Intelligence Unit (FIU-IND) could expand its role with stronger statutory powers and technological capacity.

Whistleblower protection is another area where the US system is considered particularly effective. The Securities and Exchange Commission (SEC) operates a whistleblower programme that offers financial rewards to individuals who provide original information leading to successful enforcement action. This has significantly improved the detection of securities fraud and corporate misconduct. India's whistleblower framework, by comparison, remains relatively limited.

Although the Whistle Blowers Protection Act, 2014 provides some safeguards, it does not offer the kind of financial incentives or institutional support seen in the US system. The act would benefit from specific legislative reforms, including:

Stronger protections against retaliation, including criminal penalties for employers who victimise whistleblowers

The extension of the Act's coverage to the private sector (the current Act primarily applies to public sector disclosures)

The establishment of a dedicated whistleblower authority with investigative and oversight powers

Time-bound requirements for the investigation of complaints filed under the Act, to prevent indefinite pendency.

United Kingdom (UK)

The UK has developed a number of legal and institutional approaches that are often seen as useful models for strengthening fraud enforcement systems like India's.

One of the key strengths of the UK framework is the Fraud Act 2006, which brings different forms of fraud under a single, clear definition. Instead of relying on multiple scattered offences, it defines fraud in three broad ways: false representation, failing to disclose information, and abuse of position. This makes the law more flexible and easier to apply to modern forms of fraud, including those involving digital platforms and emerging technologies such as AI.

The UK also relies heavily on specialised institutions such as the Serious Fraud Office (SFO), which combines investigative and prosecutorial powers within a single agency. This structure allows for more coordinated and technically informed handling of complex financial crime cases. In addition, recent reforms under the Economic Crime and Corporate Transparency Act, 2023, have introduced a "failure to prevent fraud" offence. This means that large organisations can be held criminally responsible if they do not have reasonable systems in place to prevent fraud committed by their employees or associates, even if senior management was not directly involved. The law also has strong extraterritorial reach, reflecting the reality that corporate fraud often crosses borders and involves offshore entities.

Another important tool in the UK system is the Unexplained Wealth Order (UWO), introduced under the Criminal Finances Act, 2017. This allows authorities to require individuals to explain the source of their wealth when there are reasonable grounds to suspect that their assets are disproportionate to their known income. It shifts the burden of explanation in certain high-risk cases and supports faster asset tracing and recovery. The UK is also a signatory to the Budapest Convention on Cybercrime, which helps streamline cross-border access to electronic evidence and strengthens international cooperation in cyber and financial crime investigations.

Most significantly, the UK Crime and Policing Act, 2026, which comes into effect in June 2026 pursuant to the foundations laid by the Economic Crime and Corporate Transparency Act 2023, has substantially expanded the criminal prosecution of corporations in the UK. This development marks a significant shift from traditional principles of corporate criminal liability, which historically limited attribution of criminal intent to corporations except in cases involving the acts of individuals constituting the company's "directing mind and will".

The UK Crime and Policing Act 2026 addresses the mens rea problem through the doctrine of "identification": the criminal intention of a "senior manager", defined broadly to include any individual who plays a significant role in making decisions about how the whole or a substantial part of the company's activities are managed or organised, is attributed to the company itself. The Act therefore moves away from the restrictive "directing mind and will" test, which previously required the prosecution to identify the guilty mind of the most senior controlling officer of the company, and adopts a broader managerial identification standard that is more readily applicable to large, complex corporate structures.

Taken together, these international models demonstrate that modern anti-fraud frameworks increasingly rely upon three common features: specialised enforcement institutions, incentivised corporate cooperation, and technology-driven financial intelligence systems. As India continues to modernise its own enforcement architecture, these approaches offer important reference points for future reform.

Overall, these measures show a stronger emphasis on unified offences, proactive corporate accountability, and faster asset recovery tools, all of which offer useful reference points for India as it continues to refine its own fraud enforcement framework.

Singapore

Singapore's Online Criminal Harms Act 2023 (OCHA) provides a useful international example for the use of content-blocking powers to prevent the spread of online fraud. The Act empowers designated authorities to direct online platforms and social media services to remove harmful content or restrict access to their services when those services are being used for criminal activity. Singapore law enforcement agencies have invoked these powers to stop the spread of deepfake fraud, online impersonations of government officials, and other technology-enabled scams.

In an operation with global police co-operation agency INTERPOL, the Anti-Scam Command (ASCom), which consolidates resources and expertise across all police units in Singapore, investigated over 2,000 individuals and froze more than 5,300 bank accounts in Singapore, recovering more than $11.5m.[14]

India has an analogous statutory power under Section 69A of the Information Technology Act, 2000 read with Rule 16 of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Section 69A empowers the Central Government to direct any internet intermediary to block access to any information where it is necessary or expedient to do so in the interest of preventing the incitement of cognisable offences.

However, unlike Singapore's OCHA, which confers direct platform-direction powers on law enforcement, India's Section 69A mechanism routes all blocking orders through the Central Government (MeitY), and the Supreme Court in the case of Dhyan Foundation v. Google LLC & Anr., SLP (Crl.) 2497/2026 has confirmed that Magistrates and criminal courts have no independent jurisdiction to order removal or blocking of online content and that Section 69A constitutes the exclusive and self-contained statutory mechanism, with blocking powers exercisable only through the Central Government's designated authority.[15] While this framework provides procedural safeguards, the centralised approval mechanism may reduce the speed and operational flexibility required for real-time intervention in rapidly spreading online fraud campaigns.

[14] *Melvin Loh, Mediating Online Criminal Harms through the Law dated 08 April 2025 (available at: https://journalsonline.academypublishing.org.sg/Journals/SAL-Practitioner/Technology/ctl/eFirstSALPDFJournalView/mid/595/ArticleId/2044/Citation/JournalsOnlinePDF)*
[15] *Order dated 19 February 2026, Dhyan Foundation v. Google LLC & Anr., SLP (Crl.) 2497/2026*

08

Conclusion

India is currently at a very important moment in how it deals with fraud. The problem is no longer just about isolated financial crimes; it is becoming a broader challenge that affects the economy, investor trust, and how strongly people believe in the fairness of the system. When laws and enforcement mechanisms do not keep pace with new types of fraud, the costs quietly build up over time in the form of financial losses and weakened confidence in markets and institutions.

The reforms discussed in this paper are not just technical or legal adjustments. At a deeper level, they are about strengthening the systems that protect money, businesses, and public trust. They are aimed at making India's financial ecosystem more secure and better prepared for the kinds of risks that are emerging today, especially those driven by technology and cross-border activity.

To move forward, change is needed in three connected areas. Laws must be updated so they are clearer and better suited to modern fraud patterns. Enforcement agencies need stronger coordination, better tools, and more capacity so that laws are not just written but effectively applied. At the same time, companies need to take responsibility more seriously by building stronger internal systems and treating fraud prevention as part of core business discipline, not just compliance paperwork.

Equally important is the need for stronger preventive governance systems within corporations themselves. As enforcement

agencies increasingly focus on auditor accountability, ESG disclosures, internal controls, whistleblower frameworks, and governance failures, fraud prevention can no longer be treated merely as a legal compliance function. It must become an integral component of corporate risk management and institutional culture.

As financial fraud increasingly transcends national borders, effective international cooperation has become crucial for meaningful enforcement and recovery efforts. Collaborative action between countries helps trace misappropriated funds, secure assets, and strengthen accountability in complex cross-border fraud cases.

A notable recent example of successful international cooperation in anti-money laundering matters is Govt of Canada v. Sanjay Madan & Ors., CS (OS) 379/2025. The case concerned Mr. Sanjay Madan, a former senior official in the Ministry of Education, Government of Canada, who was alleged to have misappropriated university funds and channelled the proceeds into the purchase of properties in India. To recover the diverted funds, the Canadian Government initiated civil proceedings before the Delhi High Court seeking enforcement of a settlement amount representing the embezzled money.

The Delhi High Court granted interim relief by freezing Sanjay Madan's bank accounts in India and directing the concerned banks to remit approximately INR 65.9 crore to the Government of Canada towards satisfaction of the settlement amount.[16] The case serves as an important illustration of effective civil judicial cooperation between countries in anti-money laundering and fraud-related matters, distinct from the traditional Mutual Legal Assistance Treaty (MLAT) framework used in criminal proceedings. It also demonstrates the willingness of Indian courts to facilitate meaningful civil remedies in support of foreign governments pursuing anti-fraud and asset recovery actions.

Ultimately, the future effectiveness of India's anti-fraud framework will depend not merely on stronger laws, but on the ability of institutions to respond with speed, technical sophistication, and coordinated enforcement. As fraud increasingly becomes digital, borderless, and technology-driven, India's legal and regulatory architecture must evolve from a reactive model of enforcement to a proactive and intelligence-led system of prevention.

[16] *Order dated 23 June 2025, Government of Canada v. Sanjay Madan & Ors., CS (OS) 379/2025*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with 1300+ legal professionals, including 340+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com

Editorial Team

Manavendra Mishra
Partner
Dispute Resolution
manavendra.mishra@khaitanco.com

Amey Mirajkar
Partner
Dispute Resolution
amey.mirajkar@khaitanco.com

Soumyadip Ghorai
Associate
Dispute Resolution
soumyadip.ghorai@khaitanco.com

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialization, and its emergence as one of the most rapidly growing global economies. A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies. FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

Contributors

Sumeet Gupta
Deputy Secretary General
FICCI

Akhil Gupta
Director
FICCI
akhil.gupta@ficci.com

Aastha Gupta
Senior Assistant Director
FICCI
aastha.gupta@ficci.com