2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-24

CORPORATE FRAUD: ANALYZING PREVENTIVE MEASURES UNDER INDIAN LAW

Ritu Sharma*[1] Priyanka Gehlot[2]

Jaipur, Rajasthan.

Article Received: 31 March 2026
Article Revised: 21 April 2026
Published on: 11 May 2026

***Corresponding Author: Ritu Sharma**
Jaipur, Rajasthan.

DOI: https://doi-doi.org/101555/ijrpa.3174

ABSTRACT

Corporate fraud in India has evolved from a problem of episodic accounting manipulation into a broader governance, disclosure, audit, cyber, and market-integrity challenge. The modern Indian regulatory response no longer treats fraud as a matter to be addressed only after collapse. It increasingly relies on ex ante prevention through board responsibility, internal financial controls, audit committee oversight, statutory auditor reporting, specialized investigation by the Serious Fraud Investigation Office (SFIO), disciplinary action by the National Financial Reporting Authority (NFRA), disclosure-driven surveillance under the Securities and Exchange Board of India (SEBI), and risk-based compliance requirements issued by the Reserve Bank of India (RBI). This paper analyses the preventive architecture of Indian law and evaluates whether the existing framework is sufficiently integrated, credible, and future-ready. The paper combines doctrinal analysis with recent public data from SFIO, NFRA, RBI, and SEBI-related regulatory materials. The evidence shows that India has moved toward a multi-agency model of prevention, but implementation remains uneven. Stronger statutory duties exist on paper, yet their effect depends on data quality, auditor independence, continuous monitoring, whistleblower trust, cyber resilience, and inter-regulator coordination. Recent RBI fraud-risk rules and SEBI's 2024 cybersecurity framework demonstrate a decisive preventive turn, while SFIO and NFRA trends indicate that enforcement visibility has improved. Even so, recurrent spikes in reported fraud value, audit failures in high-profile entities, and the continuing dependence on post-facto investigations show that deterrence is not yet fully internalised within Indian corporate practice. The paper argues that the next stage of reform should focus on governance quality,

[1] LLM Student, Jagannath University, Jaipur
[2] Assistant Professor, Jagannath University, Jaipur

real-time red-flag analytics, stronger whistleblower assurance, consistent treatment of related-party and beneficial ownership risks, and deeper convergence between company law, securities regulation, audit regulation, and banking supervision.

KEYWORDS: Corporate fraud; Indian law; Companies Act, 2013; SFIO; NFRA; SEBI; RBI; fraud prevention; audit regulation; corporate governance.

1. INTRODUCTION

Corporate fraud has become one of the most consequential threats to investor confidence, lender discipline, market integrity, and public trust in business institutions. In the Indian setting, the subject is no longer limited to classic accounting falsification or embezzlement. It includes diversion of funds, related-party abuse, insider trading, concealment of beneficial ownership, cyber-enabled manipulation, false financial reporting, non-disclosure of material information, and the strategic use of complex organisational structures to avoid detection. What unites these forms is the abuse of corporate form for private advantage through deception, concealment, or reckless disregard of legal duties.

The significance of the problem lies in its multiplier effect. A fraudulent company can distort credit allocation, mislead minority shareholders, trigger governance contagion across groups, and weaken the credibility of auditors, directors, intermediaries, and regulators. Fraud therefore cannot be understood only as a private dispute between a company and its stakeholders. It is a systemic issue with macroeconomic, institutional, and normative consequences. It raises a central legal question: whether Indian law merely punishes fraud after exposure, or whether it is capable of preventing fraud before large-scale harm materialises.

Indian law has progressively moved toward a preventive model. The Companies Act, 2013 embeds board accountability, internal financial control obligations, committee-based monitoring, auditor reporting responsibilities, and a specialised fraud investigation mechanism. The National Financial Reporting Authority now performs a visible disciplinary and oversight role in the audit ecosystem. SEBI has strengthened disclosure, surveillance, market-conduct, insider-trading and cybersecurity expectations for listed entities and regulated intermediaries. The RBI has similarly shifted from reactive fraud reporting to

structured fraud risk management in regulated entities. These developments show that prevention is no longer incidental; it is a stated regulatory objective. [3] [4] [5]

Yet prevention is more demanding than punishment. Punishment is episodic and retrospective. Prevention requires institutional design, high-quality reporting, early warning systems, ethical incentives, functional audit committees, independent auditors, effective whistleblower channels, and regulatory coordination across silos. [6] A fraud framework may appear formidable on paper while still underperforming in practice if detection lags are long, if internal alerts are suppressed, if compliance becomes box-ticking, or if agencies act sequentially rather than jointly.

This paper studies preventive measures under Indian law through a combined doctrinal and evidence-based approach. It examines the legal architecture, the role of key institutions, recent enforcement indicators, and current implementation gaps. The argument advanced is that Indian law has built a credible preventive scaffold, but the system still needs better integration, more consistent supervisory follow-through, and stronger organisational incentives for early disclosure and internal challenge.

2. METHOD AND SCOPE

Methodologically, the paper adopts a doctrinal-analytical approach supplemented by recent institutional data. The doctrinal part examines the structure and interaction of statutory provisions, regulatory instruments, and enforcement bodies. The empirical part does not attempt to estimate the full incidence of corporate fraud in India, which would require access to private complaints, internal investigations, and entity-level supervisory data. Instead, it uses publicly available indicators that are legally meaningful: SFIO investigations completed, NFRA debarment actions, recent RBI fraud figures, and RBI penalty distributions by regulated-entity type. This mixed approach is appropriate because fraud prevention is both a legal design problem and an institutional-performance problem.

The scope of the paper is intentionally preventive rather than purely criminal. Corporate fraud can be analysed through criminal prosecution, evidence law, sentencing, insolvency

[3] Government of India. (n.d.). The Companies Act, 2013. India Code. Retrieved April 23, 2026, from https://www.indiacode.nic.in/handle/123456789/2114?sam_handle=123456789%2F1362

[4] Securities and Exchange Board of India. (2024). Cybersecurity and cyber resilience framework (CSCRF) for SEBI regulated entities (REs). Retrieved April 23, 2026, from https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

[5] Reserve Bank of India. (2024). Master directions on fraud risk management in regulated entities (REs), 2024. Retrieved April 23, 2026, from https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12702

[6] National Financial Reporting Authority. (2025a). Annual report 2023-24. Retrieved April 23, 2026, from https://nfra.gov.in/publication/annual-report-2023-24/

spillovers, or comparative regulation. Those questions are important, but they are not the core concern here. The present inquiry asks a narrower and more policy-relevant question: whether Indian law generates sufficiently strong checks before fraud causes large-scale loss, panic, or litigation. For that reason, greater attention is paid to governance processes, audit design, supervisory frameworks, and disclosure mechanisms than to trial-stage adjudication.

The data discussed in the paper should also be read as signalling devices rather than exhaustive national totals. For example, SFIO handles only serious and assigned cases; its output does not capture all fraud matters pursued through other agencies or private proceedings. NFRA's debarment list captures disciplinary visibility in the audit domain, not all instances of audit weakness. RBI fraud numbers reflect the logic of reporting and classification in regulated entities and may include lagged recognition. These limits are not defects in the paper's method. They are inherent features of fraud analysis, where official statistics often reveal more about institutional detection than about the complete universe of misconduct.

3. Conceptual Foundations of Corporate Fraud

Corporate fraud is best understood as intentional or reckless deception carried out through or within a corporate structure in order to obtain unlawful gain, conceal loss, evade duty, manipulate perception, or misdirect property, credit, or voting power. In legal analysis, the concept overlaps with misstatement, cheating, breach of fiduciary duty, market abuse, insider dealing, false certification, and unlawful diversion of funds. In governance analysis, it is linked to the misuse of authority, information asymmetry, weak controls, and skewed incentives.

The classic literature on fraud explains such conduct through opportunity, pressure, rationalisation, and capability. These behavioural insights remain relevant because most large corporate frauds do not arise from a single weak rule. They arise when a permissive environment allows managerial dominance, weak board challenge, fragmented data, poor documentation, or compromised audit independence. Recent scholarship on the fraud triangle in the Indian context reinforces the point that formal rules alone are insufficient unless institutions also pay attention to behavioural red flags, incentive structures, and contextual signals in the audited entity (Sandhu & Saluja, 2023). [7]

[7] Sandhu, N., & Saluja, S. (2023). Fraud triangle as an audit tool. Management and Labour Studies, 48(3). https://doi.org/10.1177/0258042X231160970

For present purposes, four categories of corporate fraud are especially important in India. The first is financial reporting fraud, which includes revenue inflation, concealment of liabilities, sham transactions, off-balance-sheet masking, and impairment manipulation. The second is governance fraud, which includes related-party tunnelling, siphoning of funds, round-tripping, false board processes, and abuse of promoter control. The third is market-facing fraud, such as insider trading, selective disclosure, and manipulative or unfair trade practices. The fourth is cyber-enabled or operational fraud, where digital systems, onboarding processes, or control failures facilitate unauthorised transactions, fake accounts, mule structures, or data abuse.

A serious preventive framework must therefore address more than one layer of conduct. It must regulate incentives inside the firm, the quality of financial reporting, the role of auditors and compliance officers, the integrity of market disclosures, and the resilience of digital systems. Indian law increasingly reflects this multi-layered understanding.

In N. Narayanan v. Adjudicating Officer, SEBI, (2013) 12 SCC 152, the Supreme Court ruled that, in the context of the securities market, reporting inflated profits, fabricated revenues, and presenting overstated and misleading financial statements is misleading disclosure that reduces the market's trust. Such reporting may potentially attract the public to invest in a securities market by creating a misleading perception of a company's actual performance. The decision in this case is pertinent to this paper as it demonstrates that financial reporting that constitutes fraud cannot be construed as a mere wrongful act of exercising a company's internal control over accounting. Such reporting has the potential of being a wrongful act of undermining the integrity of the market, as it influences the investors and the price of shares. [8]

4. Preventive Architecture Under Indian Law

The Companies Act, 2013 remains the centrepiece of the Indian anti-fraud framework. Its preventive logic is distributed across governance, disclosure, audit, investigation, and sanction provisions. The statute does not wait for fraud to mature into a criminal conviction before imposing responsibility. Directors must ensure proper systems, approve reliable accounts, and maintain internal controls. Auditors must examine and report. Committees must monitor. When suspicion crosses a threshold, specialised investigation can be triggered. At the back end lies a strong sanctioning regime for fraud and false statements.

[8] N. Narayanan v. Adjudicating Officer, SEBI, (2013) 12 SCC 152.

The board responsibility statement under section 134(5) is foundational because it converts fraud prevention from a purely managerial concern into a board-level legal duty. Directors are expected to confirm that accounting policies have been applied consistently and prudently, that proper and sufficient care has been taken for maintenance of adequate accounting records, and that internal financial controls are in place and operating effectively. Read with financial statement duties under sections 129 and 134, the law places truthfulness of corporate reporting squarely within the governance domain rather than treating it as a matter left entirely to auditors. [9]

Section 177, which requires an audit committee for specified classes of companies and supports a vigil mechanism, is another preventive anchor. The audit committee is not merely a forum for reviewing annual accounts. In a robust reading, it is the board's specialised anti-fraud nerve centre. It should interrogate risk concentrations, related-party exposures, auditor observations, control breaches, and the quality of remediation. Where the committee is active and independent, fraud opportunity narrows because management discretion is exposed to structured challenge. Where it is ceremonial, the statutory design loses much of its preventive force.

The ruling in N. Narayanan reinforces the proactive interpretation of board obligations. The Court pointed out that directors of listed companies have strict obligations concerning the accounts and disclosures and cannot regard financial statements as a matter of management or auditors. Within the Indian proactive framework, this fact advocates for a more robust audit committee culture, as directors should actively evaluate and verify if corporate disclosures are truthful and fair, as opposed to merely endorsing the management narratives.

The statutory auditor's role is equally central. Section 143(12) requires the auditor to report fraud to the Central Government in prescribed cases, and CARO 2020 expands the reporting environment by requiring specific comments on whether fraud by the company or on the company has been noticed or reported during the year and whether any report under section 143(12) has been filed. These requirements push fraud issues into formal audit reporting and increase the costs of silence. The deeper importance of CARO 2020 lies not in its formality but in its capacity to make fraud indicators auditable, documentable, and reviewable. [10]

In the case of Union of India v. Deloitte Haskins and Sells LLP, Criminal Appeal Nos. 2305-2307 of 2022 (Supreme Court of India, 2023), based on IL&FS, the Supreme Court ruled that

[9] Government of India. (n.d.). The Companies Act, 2013. India Code. Retrieved April 23, 2026, from https://www.indiacode.nic.in/handle/123456789/2114?sam_handle=123456789%2F1362

[10] Government of India. (n.d.). The Companies Act, 2013; Companies (Auditor's Report) Order, 2020, read with section 143(12) of the Companies Act, 2013.

the Proceedings under section 140(5) of the Companies Act, 2013 are not deemed to have been terminated because the auditor resigns. This is important from the point of view of fraud, as this court ruling implies that resigning from the audit will not be taken as a strategic option to escape serious and collusion audit-failure allegations after the statutory process has been undertaken. [11]

Sections 447, 448 and 449 supply the deterrent edge. Section 447 prescribes punishment for fraud, while sections 448 and 449 address false statements and false evidence. These provisions matter preventively because they signal that deception in corporate documentation, certification, or testimony attracts serious consequences. The legal message is that fraud is not a peripheral compliance event but a core attack on the integrity of the corporate reporting system.

Section 212 strengthens prevention through the possibility of SFIO investigation in serious cases. A specialised, multidisciplinary investigation body changes the incentive landscape for boards, key managerial personnel, auditors and intermediaries. Even before final prosecution, the prospect of forensic investigation can increase caution in documentation, approvals, and disclosure practices. The SFIO's recent output, discussed later in this paper, shows that the institution remains a visible part of the Indian anti-fraud ecosystem. [12]

In Serious Fraud Investigation Office v. Rahul Modi[13], the Supreme Court described the special characteristics of an SFIO investigation under section 212 of the Companies Act, 2013. The case is significant as it demonstrates that serious corporate fraud involves complex investigation models as opposed to simple, fragmented inquiries. This lends support to the paper's claim that prevention is reliant on credible investigation and the prompt transferring of documents to appropriate agencies, not solely on punitive measures. [14]

In Serious Fraud Investigation Office v. Nittin Johari, Criminal Appeal No. 1381 of 2019, the Supreme Court noted allegations of Bhushan Steel, a company with an extensive operation with 157 subsidiary companies, on the manipulation of account books, fraudulent letters of credit, and the significant financial loss to creditors. Although the order pertained to bail, the factual background of the order describes the mechanisms of conduct to perpetrate a crime of fraud through group subsidiaries, financial statements, the functions of the finance committee

[11] Union of India v. Deloitte Haskins and Sells LLP, Criminal Appeal Nos. 2305-2307 of 2022 (Supreme Court of India, 2023).
[12] Serious Fraud Investigation Office. (2026). Investigations completed. Retrieved April 23, 2026, from https://sfio.gov.in/en/investigation-completed/
[13] (2019) 5 SCC 266
[14] Serious Fraud Investigation Office v. Rahul Modi, (2019) 5 SCC 266.

of the board, and the channels of bank credit. The case further proves the necessity of lending monitoring, board documentation, and lending discipline. [15]

NFRA, established under section 132 of the Companies Act, adds an additional preventive layer by disciplining auditors and audit firms and by reviewing audit quality. Its presence is crucial because corporate fraud often survives not only because managers deceive, but also because assurance functions underperform. Where audit quality is weak, financial reporting becomes easier to manipulate. NFRA's expanding enforcement profile therefore has preventive significance beyond individual cases; it shapes expectations for the entire profession. [16]

For listed entities, company law prevention is supplemented by securities regulation. SEBI's LODR regime makes continuous disclosure, related-party oversight, governance committee functioning, and certification of internal controls central to listed-company compliance. This is not merely procedural disclosure law. Timely and complete disclosure reduces the space in which fraud can remain hidden behind information asymmetry. Similarly, the SEBI insider trading framework targets misuse of unpublished price sensitive information and reinforces internal codes, digital controls, structured databases, and compliance oversight. [17][18]

Sahara India Real Estate Corporation Ltd. v. SEBI, (2013) 1 SCC 1, contributes to the understanding of the role of disclosures within the framework of fraud prevention. The Court observed the Securities Exchange Board of India's power on all forms of public offering of solicitation of funds through securities. The Court stressed that, in securing the public's funds, the companies broad reliance on the form of funds offered should not be a basis to escape the regulation of the securities market. The decision illustrates the case of the rationale of disclosure, oversight of prospectus, and the protection of investors, particularly when the investors are in a condition of information asymmetry. [19]

---

[15] Serious Fraud Investigation Office v. Nittin Johari, Criminal Appeal No. 1381 of 2019 (Supreme Court of India).

[16] National Financial Reporting Authority. (2025b). Debarments. Retrieved April 23, 2026, from https://nfra.gov.in/debar/

[17] Securities and Exchange Board of India. (2026). Master circular for compliance with the provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 by listed entities. Retrieved April 23, 2026, from https://www.sebi.gov.in/legal/master-circulars/jan-2026/master-circular-for-compliance-with-the-provisions-of-the-securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-regulations-2015-by-listed-entities_99432.html

[18] Securities and Exchange Board of India. (2025). Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 [Last amended on March 12, 2025]. Retrieved April 23, 2026, from https://www.sebi.gov.in/legal/regulations/mar-2025/securities-and-exchange-board-of-india-prohibition-of-insider-trading-regulations-2015-last-amended-on-march-12-2025-_92672.html

[19] Sahara India Real Estate Corporation Ltd. v. SEBI, (2013) 1 SCC 1.

SEBI v. Kanaiyalal Baldevbhai Patel, (2017) 15 SCC 1, and SEBI v. Rakhi Trading Pvt. Ltd., (2018) 13 SCC 753, expand the scope of market fraud. These cases establish that practices such as unfair trade, frontrunning, synchronized or non-genuine trades, and trades executed for the sole purpose of market manipulation can be detrimental to market integrity, even if such practices do not qualify as standard cases of accounting fraud. Given the scope of this paper, these cases illustrate that the prevention of corporate fraud should include both market behavior and issuer-level market disclosures. [20]

A notable modern development is the increasing recognition that fraud prevention is inseparable from cyber resilience. SEBI's 2024 Cybersecurity and Cyber Resilience Framework for regulated entities reflects a shift from narrow IT compliance to institution-wide resilience. Fraud today may be executed through system compromise, access abuse, identity manipulation, or data exfiltration. Cyber controls therefore perform a legal as well as technological function: they preserve the evidentiary reliability and transactional integrity on which anti-fraud enforcement depends. [21]

The banking and financial sector reveals an even clearer preventive turn. RBI's 2024 Master Directions on Fraud Risk Management in Regulated Entities emphasise risk-based monitoring, governance responsibility, structured escalation, special board or executive committees for monitoring fraud cases, early warning signals, and tighter institutional accountability. The accompanying 2025 FAQ clarifies governance thresholds and operational expectations. This is a major conceptual shift. Fraud is treated not merely as an irregularity to be reported after discovery, but as a risk category requiring board-backed control architecture. [22]

When read together, these legal instruments show that Indian law now treats fraud prevention as a distributed responsibility. Boards, audit committees, internal auditors, statutory auditors, company secretaries, market intermediaries, regulated financial entities, and specialised agencies all form part of the protective design. The key question is whether this design is operating with sufficient consistency and speed. Table 1 summarises the current preventive architecture.

[20] SEBI v. Kanaiyalal Baldevbhai Patel, (2017) 15 SCC 1; SEBI v. Rakhi Trading Pvt. Ltd., (2018) 13 SCC 753.

[21] Securities and Exchange Board of India. (2024). Cybersecurity and cyber resilience framework (CSCRF) for SEBI regulated entities (REs). Retrieved April 23, 2026, from https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

[22] Reserve Bank of India. (2025). FAQs on master directions on fraud risk management in regulated entities (REs), 2024. Retrieved April 23, 2026, from https://www.rbi.org.in/commonman/Upload/English/FAQs/PDFs/RISK22042025.pdf

Table 1. Current preventive architecture against corporate fraud under Indian law.

Instrument	Core preventive function	How it works preventively	Practical significance
Companies Act, 2013 (ss. 134(5), 177, 212, 447–449)	Board responsibility, vigil mechanism, specialised investigation, and fraud penalties	Prevention is embedded in governance, reporting, and sanction design rather than being left only to criminal prosecution.	Board ownership of controls and truthful reporting remains the first legal defence against fraud.
Companies (Auditor's Report) Order, 2020	Expanded auditor reporting, including reporting of fraud noticed or reported during the year and reporting under s.143(12)	Raises visibility of fraud indicators and makes silence harder to sustain.	Improves audit transparency and strengthens documentary traceability.
NFRA disciplinary and oversight framework	Audit-quality oversight, disciplinary orders, debarments, inspections	Targets gatekeeper failure and enhances deterrence in the audit profession.	Signals that weak assurance can itself attract consequences.
SEBI LODR framework (current master circular)	Continuous disclosure, governance committees, certification and compliance structures for listed entities	Reduces concealment space in listed companies by forcing earlier and broader disclosure.	Useful against related-party abuse, disclosure delay, and governance opacity.
SEBI PIT Regulations (as amended to Mar. 12, 2025)	Codes of conduct, structured digital databases, UPSI controls, and informant-based enforcement architecture	Directly addresses trading and disclosure abuse rooted in information asymmetry.	Prevents misuse of price-sensitive information and reinforces compliance documentation.
SEBI CSCRF for regulated entities (2024)	Cybersecurity, resilience, governance, incident response, and control standards	Treats cyber weakness as a fraud-enabling vulnerability, not merely an IT issue.	Essential for preventing data manipulation and unauthorised transactions.
RBI Master Directions on Fraud Risk Management in REs, 2024	Risk-based fraud governance, early warning mechanisms, committees for monitoring fraud cases, escalation and follow-up	Moves regulated entities from reactive reporting to structured prevention and monitoring.	Shows the strongest current shift toward ex ante fraud control.

Interpretation: Table 1 shows that Indian anti-fraud law is no longer dependent on a single penal provision. The preventive system is layered. The Companies Act addresses governance design, board responsibility, internal control and investigation; CARO 2020 adds audit-report visibility; NFRA addresses audit quality and professional discipline; SEBI addresses listed-entity disclosures, insider-trading controls and cyber resilience; and RBI applies risk-based fraud governance to financial entities. The principal strength of the framework is breadth. The principal weakness is fragmentation. Because fraud can move across governance, audit, banking and securities domains, the effectiveness of the framework depends less on the existence of each instrument in isolation and more on whether signals move quickly between them.

5. Recent Institutional and Enforcement Trends

Preventive law is best evaluated not only by textual strength but also by recent institutional patterns. Three indicators are especially useful for present purposes: specialised corporate-fraud investigations completed by SFIO, audit-regulator disciplinary visibility through NFRA, and banking-sector fraud and penalty data linked to the RBI. These indicators do not measure the entire fraud universe. They do, however, show whether the Indian system is becoming more interventionist, more transparent, and more capable of sending preventive signals to firms and gatekeepers.

The data must be interpreted with care. Reported fraud cases and reported fraud value may move in opposite directions because detection and reporting often lag the underlying misconduct. A fall in the number of reported cases does not necessarily imply that fraud risk has fallen; it may reflect classification changes, reporting thresholds, or the unwinding of earlier reclassifications. Conversely, a spike in reported value may result partly from delayed recognition of legacy cases. This reporting lag is particularly important in interpreting RBI data for 2024-25.

Table 2. RBI-reported bank fraud trend in India

Financial year	Reported fraud cases	Amount involved (Rs crore)	Analytical note
2022-23	13,564	26,127	FY2022-23 forms the pre-surge base year in the present trend series.
2023-24	36,075	13,930	FY2023-24 saw a sharp rise in reported cases but a decline in value, showing that case volume and loss severity do not move together.

2024-25	23,953	36,014	FY2024-25 saw fewer reported cases but a steep jump in value, reflecting delayed recognition and higher-value exposures.

Interpretation: Table 2 reveals a pattern that is highly relevant to preventive law. The number of reported bank fraud cases rose sharply in 2023-24, fell in 2024-25, yet the amount involved rose steeply in 2024-25. This divergence suggests that raw case counts are an inadequate proxy for underlying risk. Higher-value frauds, delayed recognition, and reclassification can change the loss profile even when case numbers moderate. From a legal-policy perspective, this means prevention cannot rely on annual incident counting alone. Boards and regulators need granular risk segmentation by product, exposure class, control failure, and time-to-detection. [23][24]

Table 3. Selected institutional enforcement indicators.

Panel A: SFIO financial year	Investigations completed	Panel B: NFRA calendar year	Debarment entries
2019-20	12	2022	3
2020-21	7	2023	64
2021-22	13	2024	35
2022-23	29	2025 (to Mar 11)	1
2023-24	18		
2024-25	22		

Interpretation: Table 3 indicates that India's institutional response to corporate misconduct is active, but uneven across agencies and time periods. SFIO's completed investigations increased from 7 in 2020-21 to 29 in 2022-23 and remained comparatively strong thereafter. NFRA's debarment activity surged in 2023 and remained substantial in 2024, underlining that audit quality enforcement has become a material feature of the anti-fraud landscape. These trends support the view that prevention in India increasingly depends on visible gatekeeper discipline. At the same time, year-to-year volatility shows that the system still reacts in waves rather than through fully stable, continuous monitoring. [25]

[23] Business Standard. (2024, May 30). Bank frauds rise 166% in FY24 to over 36,000 cases, shows RBI annual report. https://www.business-standard.com/industry/banking/bank-frauds-rise-166-in-fy24-to-over-36-000-cases-shows-rbi-annual-report-124053001237_1.html

[24] Business Standard. (2025, May 30). Bank fraud cases fell in FY25, amount rose threefold to ₹36,014 crore: RBI. https://www.business-standard.com/finance/news/bank-fraud-amount-triples-in-fy25-despite-drop-in-number-of-cases-rbi-125052900696_1.html

[25] Serious Fraud Investigation Office. (2026). Investigations completed; National Financial Reporting Authority. (2025b). Debarments.

Table 4. RBI FY2024-25 penalty distribution by regulated entity type.

Regulated entity type	Penalty count	Known penalty amount (Rs crore)
Co-operative banks	264	15.63
NBFCs / ARCs	37	7.29
Housing finance companies	13	0.83
Public sector banks	8	11.11
Private sector banks	15	14.80
Foreign banks	6	N.A.

Interpretation: Table 4 shows that RBI enforcement in FY2024-25 was dominated numerically by co-operative banks, followed by NBFCs/ARCs and housing finance companies, while the largest known penalty amounts were imposed on private and public sector banks. This suggests a dual regulatory reality. Smaller entities generate high enforcement volume, often due to repeated compliance weaknesses, whereas larger institutions account for higher-value lapses when failures occur. For preventive policy, this means one-size-fits-all supervision is suboptimal. India needs differentiated fraud-control expectations matched to entity size, business model, technology exposure, and systemic significance. [26]

6. Visual Analysis of the Recent Data

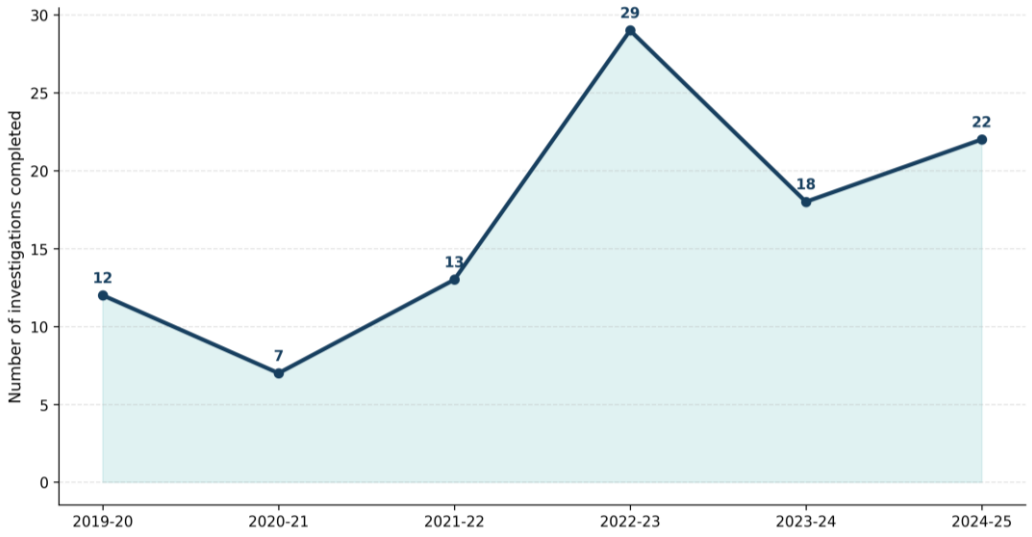

Chart 1. SFIO investigations completed by financial year.

Interpretation: Chart 1 shows that SFIO's completed investigations did not move in a flat line. The sharp rise in 2022-23 and the still-elevated numbers in 2023-24 and 2024-25 suggest that specialised corporate-fraud investigation capacity remains active after the

[26] ETBFSI. (2025, May 29). RBI imposes Rs 54.78 cr penalty in FY25 across 353 actions under Utkarsh 2.0. https://bfsi.economictimes.indiatimes.com/articles/rbis-utkarsh-20-5478-cr-penalty-imposed-in-fy25-for-compliance-violations/121481845

pandemic-era trough. This matters preventively because serious investigation capability strengthens ex ante discipline among boards and promoters. Even where prosecution is delayed, visible case throughput can improve compliance behaviour by increasing the expected cost of concealment.

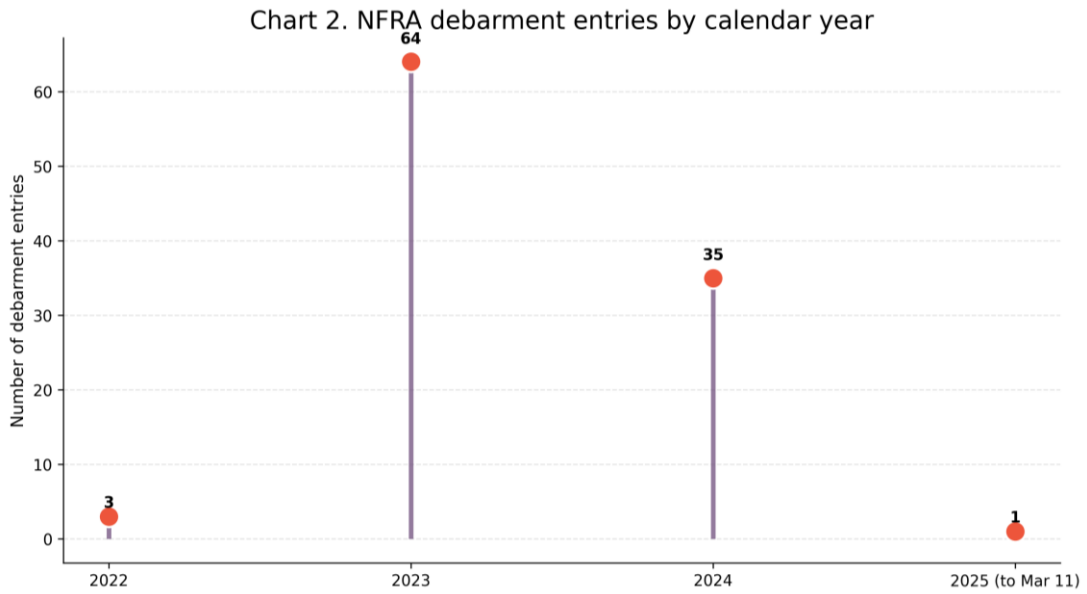

Chart 2. NFRA debarment entries by calendar year.

Interpretation: Chart 2 highlights the expansion of NFRA's disciplinary visibility. The jump from 3 debarment entries in 2022 to 64 in 2023, followed by 35 in 2024, indicates that audit regulation in India has become more assertive. This is significant because many major corporate frauds depend on failures of assurance, challenge, and professional skepticism. A more visible audit regulator improves fraud prevention indirectly by increasing the accountability of those expected to detect reporting irregularities early.

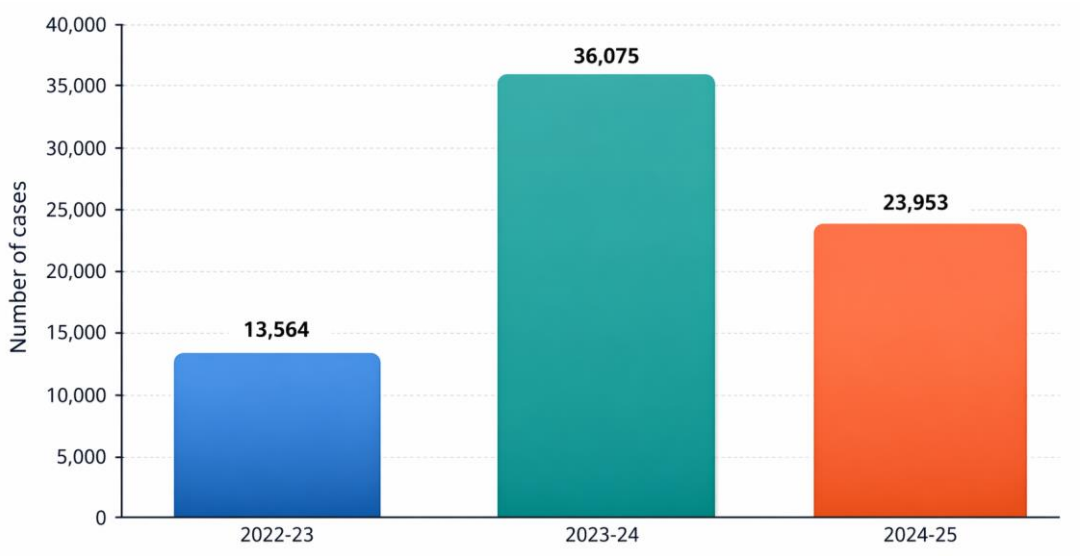

Chart 3. Reported bank fraud cases in India.

Interpretation: Chart 3 demonstrates the volatility of reported fraud incidence in the banking system. The surge in 2023-24 followed by a decline in 2024-25 does not by itself imply that the preventive framework has stabilised. A fall in cases can coexist with persistent structural weaknesses if reporting lags remain high or if fewer but larger frauds dominate the system. The chart therefore underscores the need for a prevention strategy that looks beyond aggregate annual counts.

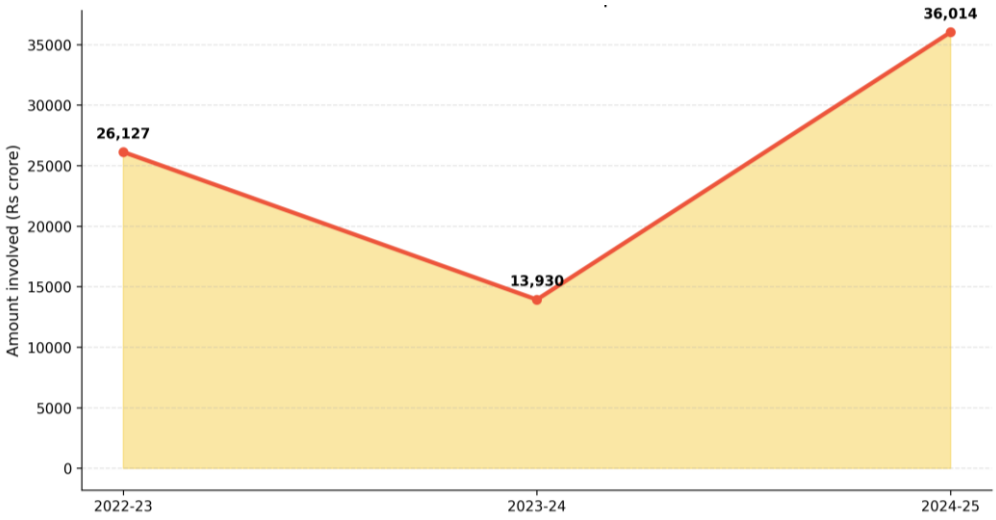

Chart 4. Amount involved in reported bank frauds.

Interpretation: Chart 4 is perhaps the most revealing chart in the paper. Fraud value fell in 2023-24 and then climbed sharply in 2024-25, despite the lower number of reported cases. This pattern strongly suggests that loss severity and detection timing matter more than volume alone. The legal implication is clear: India's anti-fraud regime must prioritise faster

detection, earlier escalation, and more credible challenge mechanisms in large exposures, especially where loan portfolios and complex structures are involved.

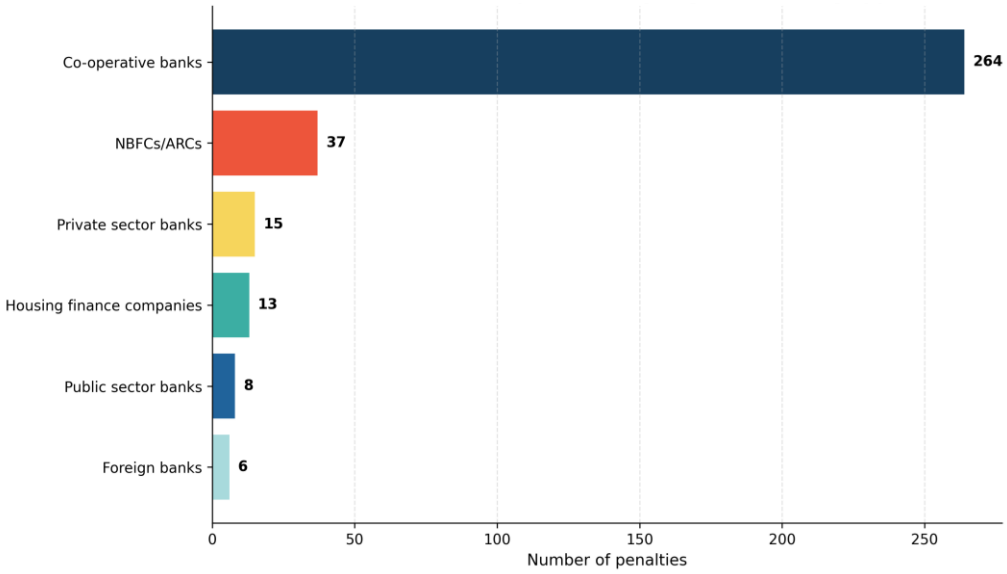

Chart 5. RBI FY2025 penalties by regulated entity type.

Interpretation: Chart 5 shows that RBI's FY2024-25 enforcement actions were heavily concentrated in co-operative banks, with a much smaller but still meaningful cluster in NBFCs/ARCs, housing finance companies, public sector banks, private sector banks, and foreign banks. The concentration of actions suggests that preventive compliance remains uneven across the regulated landscape. It also supports a risk-based supervisory model in which recurring control failures in high-volume categories are addressed through tighter governance expectations, targeted inspections, and stronger remediation follow-up.

7. Critical Evaluation of the Preventive Measures

The empirical picture suggests that India has made real progress in building a preventive ecosystem, but the quality of prevention remains contingent on how the different legal layers interact. The first strength of the present framework is that prevention is now embedded in ordinary corporate governance rather than confined to criminal investigation. Directors must certify responsibility, committees must review, auditors must report, and listed entities must disclose on a continuing basis. This architecture increases the number of institutional checkpoints at which deception may be challenged before it becomes catastrophic.

The second strength lies in the visible disciplining of gatekeepers. NFRA's debarment activity and its broader oversight role matter because fraud is often enabled by silent or

inattentive assurance structures. When auditors understand that failures of skepticism, documentation, independence, or reporting may attract serious professional consequences, the detection environment improves. The same logic applies to SEBI-regulated entities: stronger disclosure and insider-trading controls make concealment costlier.

In Securities and Exchange Board of India v. Terrascope Ventures Ltd., 2026 INSC 245, the Supreme Court intervened to restore a SEBI penalty order. This case concerns the misuse of preferential allotment funds for purposes other than those disclosed, and provides clarity on the different regulatory domains of market-access restraint and its monetary penalty. The case is relevant to the order under analysis, as it strengthens the principle of deterrence. Fraudulent conduct constitutes a severe breach of regulatory obligation, and the effectiveness of a preventive system is diminished if the only consequence is a temporary restriction. In such a case, the absence of a substantial financial penalty invites further violations. [27]

The third strength is the migration from static compliance to risk-based supervision. RBI's fraud risk management directions are especially notable for requiring regulated entities to institutionalise fraud governance rather than treat fraud as an isolated operations problem. This is a more sophisticated conception of prevention because it links board oversight, escalation, internal analytics, and response design.

Even so, important weaknesses remain. First, the Indian framework still suffers from asymmetry between formal compliance and substantive challenge. Many firms can satisfy documentary requirements without cultivating a culture of escalation, dissent, or evidentiary discipline. Fraud prevention fails when independent directors lack real information, when audit committees depend too heavily on management summaries, or when internal audit is structurally subordinate to the executives it is expected to examine.

Second, auditor duties remain powerful in law but difficult in practice. Section 143(12), CARO 2020, and NFRA oversight have strengthened expectations, yet practical independence can still be undermined by client concentration, fee dependence, delayed access to records, and the complexity of group structures. The significance of the Supreme Court-backed conversation around auditor resignation and continuing accountability is that it narrows the space for strategic exit when fraud indicators begin to surface. As Deb argues in the Indian context, auditor independence cannot be treated as a formal status alone; it is

[27] Securities and Exchange Board of India v. Terrascope Ventures Ltd., 2026 INSC 245.

integral to fraud prevention because resignation should not become a route for escaping scrutiny (Deb, 2024). [28]

Third, fraud prevention in promoter-led and closely controlled companies remains particularly challenging. Concentrated control can produce both monitoring benefits and abuse risks. Where governance is promoter-centric, related-party transactions, connected lending, layered entities, and informal decision channels may weaken the evidentiary trail. Indian law addresses parts of this problem through disclosure, audit committee review, beneficial ownership requirements, and securities law obligations, but enforcement still depends on timely data and institutional willingness to investigate complex business groups.

Fourth, cyber and digital fraud risks increasingly blur the boundary between corporate fraud, market abuse, and operational failure. The preventive response cannot therefore remain purely legalistic. It requires log integrity, access controls, maker-checker discipline, identity verification, anomaly detection, vendor risk management, and incident escalation. SEBI's 2024 CSCRF is important precisely because it recognises that digital weakness can become fraud opportunity.

Fifth, whistleblower confidence remains uneven. A preventive system functions best when insiders believe that reporting channels are confidential, responsive, and free from retaliation. The law in India has moved in this direction through vigil-mechanism requirements and securities-market informant design, but organisational culture still determines whether employees actually use these channels. Many frauds are visible internally long before they reach regulators. The core challenge is not only legal availability of a channel, but institutional credibility of protection.

Finally, inter-agency coordination remains a structural issue. A single fraud event may implicate the Companies Act, audit law, securities regulation, banking supervision, anti-money-laundering processes, and tax or forensic investigation. Yet agencies often intervene at different stages, with different evidentiary priorities, and through different procedural timelines. Preventive efficiency suffers when there is no seamless red-flag architecture across these domains.

8. Persistent Gaps in the Present Framework

A further issue concerns the jurisprudence of due process and classification. The recent regulatory conversation in banking demonstrates that fraud control must remain consistent

[28] Deb, R. (2024). Fraud prevention and auditors' resignation: Indian evidence. Metamorphosis. Advance online publication. https://doi.org/10.1177/09726225241261773

with procedural fairness. When fraud labelling or classification is revised after judicial intervention, annual data may shift in ways that reflect legal compliance rather than fresh misconduct. This does not weaken the case for prevention; it strengthens it. A preventive system should be built so that classification disputes do not delay internal controls, account monitoring, or evidentiary preservation. Procedural fairness and early risk containment must coexist rather than being treated as opposites.

Another practical weakness is the uneven quality of remediation. Many legal systems can identify control failure after the fact; fewer can ensure that the same failure does not recur. In India, remediation often depends on whether the organisation treats a fraud event as an isolated embarrassment or as a governance-learning moment. A mature preventive framework should require post-incident root-cause review, board-level tracking of corrective action, and external validation where failures are serious. Without such discipline, even strong enforcement can produce only episodic compliance.

There is also a sectoral asymmetry in fraud prevention. Listed companies, banks, and large regulated entities generally face denser compliance obligations and more frequent scrutiny. Private unlisted companies outside intensive supervisory environments may operate with weaker documentation, thinner compliance teams, and reduced external visibility until distress becomes acute. This asymmetry matters because significant fraud can incubate in less visible entities before surfacing through creditor disputes, group contagion, or capital-market exposure. The broader anti-fraud strategy should therefore not assume that preventive strength in highly regulated sectors automatically extends across the corporate economy.

9. Reform Agenda

A more effective preventive regime under Indian law should proceed along six reform lines. The first is to deepen board-level ownership of fraud risk. Audit committees should move beyond quarterly review culture toward continuous oversight of red-flag dashboards, related-party concentrations, audit qualifications, unusual journal entries, cyber incidents, and whistleblower trends. Board evaluation metrics should explicitly incorporate fraud governance, not merely financial performance or procedural attendance.

The second reform is to improve the quality of internal financial controls as living systems rather than annual certifications. Internal controls should be mapped to concrete fraud scenarios such as procurement collusion, revenue acceleration, fund diversion, ERP override, fake vendor creation, round-tripping, and insider access misuse. Law and regulation already

nudge firms in this direction, but supervisory guidance can better require scenario-based testing, not just control narratives.

The third reform is to strengthen audit independence through a more evidence-oriented approach to resignation, rotation, documentation, and communication with audit committees. The legal environment should continue to discourage the use of resignation as a shield against accountability where serious fraud indicators have already emerged. At the same time, audit committees should be required to provide more transparent public explanations when there are changes in auditors under suspicious circumstances.

The fourth reform is to build real-time analytic capacity across regulators and large companies. Fraud detection should increasingly rely on integrated data signals: related-party network mapping, beneficial-ownership analytics, transaction outliers, unusual disclosure patterns, audit trail exceptions, and cross-platform cyber indicators. India's preventive regime will remain only partially effective if it depends predominantly on ex post documentary review in a digital economy.

The fifth reform is to improve whistleblower trust architecture. Internal vigil mechanisms should guarantee anonymity options, protected escalation, independent triage, and time-bound board reporting. For listed and large companies, disclosure norms could be refined so that aggregate whistleblower statistics and closure quality become meaningful governance signals without compromising confidentiality. The stronger the internal reporting climate, the less dependent the system becomes on late-stage regulatory intervention.

The sixth reform is coordination. India would benefit from a more structured inter-regulatory fraud intelligence model linking SFIO, NFRA, SEBI, RBI, stock exchanges, and other relevant authorities through standardized red-flag protocols. Not every agency needs identical powers, but the system should ensure that a high-quality signal in one domain does not remain isolated there. A modern preventive framework is strongest when regulatory information travels faster than fraudulent adaptation.

These reforms do not require a complete redesign of Indian law. The existing statutory and regulatory foundations are already significant. The more urgent task is institutional calibration: better use of data, stronger gatekeeper accountability, more credible organisational reporting, and more coherent cross-agency response.

A final practical lesson concerns documentation discipline. Preventive law functions effectively only when organisational memory is reliable. In many fraud episodes, responsibility becomes diffused because approvals were informal, exception handling was undocumented, and key discussions took place outside auditable systems. Indian companies

therefore need retention rules that preserve board papers, committee minutes, internal investigation records, conflict disclosures, related-party justifications, and management representation trails in a form that can later be tested by regulators, auditors, and courts. The evidentiary value of documentation is not merely defensive. It is itself preventive, because decision-makers behave more cautiously when they know that future review will be possible and that explanations must be matched with contemporaneous records.

The compliance roadmap must also recognise proportionality. The anti-fraud burden cannot be designed only for the largest listed corporations. Unlisted public companies, large private companies, NBFCs, financial intermediaries, and rapidly scaling digital businesses also face material fraud risk, but they differ in size, staffing, and technological capacity. A sensible Indian approach would therefore calibrate preventive expectations without diluting core duties. Every significant company should have a minimum baseline consisting of board-level fraud oversight, channelised whistleblower intake, maker-checker controls over payments and accounting entries, conflict-of-interest declarations, and documented escalation to the audit committee or equivalent governing body. Additional expectations such as advanced data analytics, forensic monitoring tools, and integrated cyber-fraud simulation can then scale with entity complexity and public impact.

Another practical implication is that fraud prevention must be treated as an enterprise-wide governance issue rather than as a matter for the legal department alone. Experience shows that frauds often emerge in the spaces between functions: finance may notice unusual reconciliations, procurement may observe vendor concentration, compliance may detect disclosure inconsistencies, information security teams may see credential misuse, and human resources may receive behavioural complaints that do not initially appear financial. A preventive system becomes credible only when these signals are brought into one reporting architecture. The board, and especially the audit committee, should therefore require periodic integrated fraud dashboards that combine financial-control exceptions, related-party alerts, whistleblower metrics, cyber incidents with fraud implications, and status reports on internal investigations. Such integration is increasingly consistent with Indian regulatory direction, particularly as fraud risk, cyber resilience, and continuous disclosure are now more closely connected.

For publication-oriented policy analysis, the most important takeaway is that preventive success cannot be judged solely by the harshness of punishment after a scandal. A mature legal system prevents fraud by reducing opportunity, increasing the probability of early detection, and making concealment difficult at every organisational layer. Indian law already

contains many of these elements, but companies often implement them in a fragmented manner. The next stage of reform should therefore emphasise board routines, data-backed monitoring, stronger protection for internal reporting, credible auditor challenge, better coordination between corporate and sectoral regulators, and faster translation of red flags into formal action. Where these practices become routine, the law moves from symbolic deterrence to operational prevention.

10. Practical Compliance Roadmap for Companies

A practical compliance roadmap for companies should begin with board-level ownership of fraud risk, supported by an active audit committee, clear internal financial controls, and regular review of red-flag indicators. Companies should maintain effective whistleblower channels with confidentiality, prompt investigation, and protection against retaliation so that internal concerns surface before they become major violations. Fraud prevention should not remain confined to the legal department; finance, procurement, compliance, internal audit, human resources, and information security teams should operate through an integrated reporting structure. Periodic fraud dashboards should combine control exceptions, related-party alerts, cyber incidents, vendor irregularities, and investigation updates for senior oversight. Documentation is equally essential, because reliable records of approvals, disclosures, committee discussions, and conflict declarations strengthen accountability and early detection. A proportionate approach is also necessary, so that baseline anti-fraud safeguards apply across listed and unlisted entities, while advanced analytics and forensic monitoring scale with organizational complexity and risk.

11. CONCLUSION

Indian law has travelled a considerable distance from a narrow post-facto conception of corporate fraud. The present framework reflects a preventative ambition expressed through board duties, auditor reporting, specialised investigation, audit regulation, securities disclosure, insider-trading control, cyber resilience, and fraud-risk governance in financial entities. This is an important legal achievement.

At the same time, the evidence examined in this paper shows that prevention remains uneven in operation. Enforcement visibility has increased, yet reporting lags, governance formalism, audit dependence, fragmented data, and uneven supervisory intensity continue to limit deterrence. The lesson is not that Indian law lacks anti-fraud tools. It is that the tools must be used in a more integrated, intelligence-led, and institutionally credible manner.

The strongest future for Indian anti-fraud law lies in convergence: convergence between company law and securities regulation, between audit oversight and board responsibility, between fraud governance and cyber resilience, and between internal reporting systems and external supervisory response. If that convergence is pursued consistently, Indian law can shift further from reactive exposure toward genuine prevention.

REFERENCES

1. Government of India. (n.d.). The Companies Act, 2013. India Code. Retrieved April 23, 2026,from https://www.indiacode.nic.in/handle/123456789/2114?sam_handle=123456789%2F1362
2. National Financial Reporting Authority. (2025a). Annual report 2023-24. Retrieved April 23, 2026, from https://nfra.gov.in/publication/annual-report-2023-24/
3. National Financial Reporting Authority. (2025b). Debarments. Retrieved April 23, 2026, from https://nfra.gov.in/debar/
4. Reserve Bank of India. (2024). Master directions on fraud risk management in regulated entities (REs), 2024. Retrieved April 23, 2026, from https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12702
5. Reserve Bank of India. (2025). FAQs on master directions on fraud risk management in regulated entities (REs), 2024. Retrieved April 23, 2026, from https://www.rbi.org.in/commonman/Upload/English/FAQs/PDFs/RISK22042025.pdf
6. Securities and Exchange Board of India. (2024). Cybersecurity and cyber resilience framework (CSCRF) for SEBI regulated entities (REs). Retrieved April 23, 2026, from https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html
7. Securities and Exchange Board of India. (2025). Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 [Last amended on March 12, 2025]. Retrieved April 23, 2026, from https://www.sebi.gov.in/legal/regulations/mar-2025/securities-and-exchange-board-of-india-prohibition-of-insider-trading-regulations-2015-last-amended-on-march-12-2025-_92672.html
8. Securities and Exchange Board of India. (2026). Master circular for compliance with the provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 by listed entities. Retrieved April 23, 2026, from

https://www.sebi.gov.in/legal/master-circulars/jan-2026/master-circular-for-compliance-with-the-provisions-of-the-securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-regulations-2015-by-listed-entities_99432.html

9. Serious Fraud Investigation Office. (2026). Investigations completed. Retrieved April 23, 2026, from https://sfio.gov.in/en/investigation-completed/
10. Deb, R. (2024). Fraud prevention and auditors' resignation: Indian evidence. Metamorphosis. Advance online publication. https://doi.org/10.1177/09726225241261773
11. Sandhu, N., & Saluja, S. (2023). Fraud triangle as an audit tool. Management and Labour Studies, 48(3). https://doi.org/10.1177/0258042X231160970
12. Business Standard. (2024, May 30). Bank frauds rise 166% in FY24 to over 36,000 cases, shows RBI annual report. https://www.business-standard.com/industry/banking/bank-frauds-rise-166-in-fy24-to-over-36-000-cases-shows-rbi-annual-report-124053001237_1.html
13. Business Standard. (2025, May 30). Bank fraud cases fell in FY25, amount rose threefold to ₹36,014 crore: RBI. https://www.business-standard.com/finance/news/bank-fraud-amount-triples-in-fy25-despite-drop-in-number-of-cases-rbi-125052900696_1.html
14. ETBFSI. (2025, May 29). RBI imposes Rs 54.78 cr penalty in FY25 across 353 actions under Utkarsh 2.0. https://bfsi.economictimes.indiatimes.com/articles/rbis-utkarsh-20-5478-cr-penalty-imposed-in-fy25-for-compliance-violations/121481845