Role of Forensic Accounting in Detecting Corporate Frauds: A Behavioural Analysis Perspective on Narratives of Deviance in Emerging India

PAYAL TEOTIA, JYOTASANA, DINESH CHAND,
DR. MOHD SHAHID ALI, SAILU KARRE, MARY SAHA*

Abstract: *Corporate financial fraud is one of the major threats to a faster-growing economy like India. This study examines the capability of forensic accounting to detect corporate fraud and also studies the tools that can help in preventing it. For qualitative analysis, five case studies for major Indian financial fraud cases: Satyam Computers Pvt. Ltd., Punjab National Bank – Nirav Modi, IL&FS, DHFL, and Yes Bank are integrated with key behavioural fraud theories of Fraud Triangle, Fraud Diamond, and Fraud Pentagon. These theories are used to analyse the driving factors for fraud, such as pressure, opportunity, rationalisation, capability, arrogance, and competence. The major reason for large-scale manipulation and societal deviance, as revealed by the findings, includes a recurring pattern of weak internal controls, governance failures, and concentration of managerial power. Due to the compliance-oriented nature of traditional auditing mechanism, it fails to detect the early warning signals. Forensic accounting has various techniques like data analytics, transaction mapping, and behavioural risk profiling showcases strong potential for detecting early warning signals. Based on this analysis, an Integrated Behavioral Forensic Risk Framework (IBFRF) is created that links behavioral patterns with forensic accounting tools and a continuous monitoring system. The framework focuses on proactive fraud detection rather than a reactive investigative approach. This study contributes to the existing forensic accounting literature by providing a structured, application-based model with practical implications for auditors, regulators, and corporate governance systems in emerging economies.*

Payal Teotia, KCC Institute of Legal and Higher Education, Greater Noida, U.P., India.
Email: payal98chaudhary@gmail.comn ORCID ID: 0009-0008-4743-0864
Jyotasana, School of Liberal Arts and Humanities Woxsen University, Telangana, India.
Email: jyotsanacug@gmail.com ORCID ID: 0000-0001-8349-6774)
Dinesh Chand, School of Liberal Arts and Humanities, Woxsen University, Telangana, India.
Email: dinesh.chand@woxsen.edu.in ORCID ID: 0000-0002-2631-9453
Dr. Mohd Shahid Ali*, School of Management, IILM University Gurugram-122011, Haryana, India.
*Correspondence Email: mohd.shahid@iilm.edu ORCID ID: 0009-0004-9749-8366,
Sailu Karre, School of Liberal Arts & Humanities, Woxsen University, Telangana, India.
Email: sailu.k@woxsen.edu.in ORCID ID: 0009-0000-2484-3019
Mary Saha, School of Liberal Arts & Humanities ,Woxsen University, Telangana, India.
Email: mary.saha@woxsen.edu.in

Keywords: Deviance, Forensic Accounting, Emerging Economies, Corporate Governance, Fraud Detection

Introduction

The threat posed by corporate financial frauds is probably the greatest challenge faced by global economic stability, investors' confidence, and sustained economic growth in recent times. The complexity of the business environment coupled with globalisation and technological advancement has made corporate frauds more common, as well as more difficult to uncover (Rezaee & Riley, 2010, p. 28). Financial statement auditing is meant to verify the accuracy and objectivity, but several notable crises have revealed many inherent problems in the traditional system. On the other hand, forensic accounting has been widely recognized around the world as a profession that integrates accounting, auditing, investigations, law, data analysis, and psychology in order to detect, prevent, and examine fraud (DiGabriele, 2008, p. 35). Within the sociology of deviance, financial crime is key crime under white collar crimes. As Sutherland (1983, p.7 and Reurink, 2016, p.389) defined a crime committed by a person of respectability and high social status in the course of his occupation.

It is noteworthy that some of the most significant corporate scandals witnessed in the 21st century also occur in India, which is among the fastest-growing economies in the world. It is important to emphasize the main weaknesses in corporate governance structures, regulation and supervision, internal controls, and statutory audits through some of the significant corporate scandals in the country, such as the Satyam Computer Services scandal (2009), Punjab National Bank-Nirav Modi fraud (2018), the IL&FS default scandal (2018), the Dewan Housing Finance Corporation Limited scandal (2019), and the Yes Bank corporate governance scandal (2020) (Ministry of Corporate Affairs, 2019, p. 13; SEBI, 2020, p. 22; SFIO, 2021, p. 40).

Cases of fraud being perpetrated in India on a regular basis give rise to several serious issues regarding the effectiveness of financial reporting and auditing tools in preventing complex frauds. In contrast to ordinary auditing, forensic accounting involves a proactive and interrogative approach. It may uncover any risk factors for fraud, behaviours that often precede fraudulent activities, and misstatement within financial information. In addition, forensic accounting makes use of various behavioural models, such as the Fraud Triangle developed by Cressey (1953, p. 45), the Fraud Diamond developed by Wolfe and Hermanson (2004, p. 39), and the Fraud Pentagon (Crowe Horwath, 2011, p. 15).

Although the importance of forensic tools used in accounting is becoming increasingly apparent internationally, there is still very little academic literature regarding the use of forensic techniques in developing countries. Most studies have been undertaken focusing on Western regulations and developed countries, while a country such as India faces unique problems due to its different regulations and other factors (Rezaee & Riley, 2010, p. 28). This study will try to fill this gap by performing an extensive forensic analysis of the biggest corporate frauds of India. Using various models of fraud behavior as deviance, this study will analyze how various factors such as pressure, opportunity, rationalization, capability, arrogance, and competence

played their roles in committing these frauds. Moreover, this research assesses the feasibility of using forensic accounting to prevent these frauds from occurring or being further escalated. In particular, the current study seeks to address the gaps by applying three fraud models to five Indian corporate fraud cases.

Moreover, the current research enriches the policy-making process by combining case studies with well-known fraud theories and forensic approaches. The findings offer valuable insights for regulators, auditors, corporate governance committees, forensic experts, and policy makers in India and other developing nations with comparable vulnerabilities. Ultimately, the research recommends a layered forensic accounting model to enhance corporate governance and forestall any potential financial scandals in regions prone to such activities.

Review of Literature

Forensic accounting is considered a specialized branch of accounting, distinct from the general area of accounting. This is because it has grown from mere accounting into areas such as detecting fraud, helping in legal matters, and conducting investigations. Unlike an audit that verifies compliance with regulations, forensic accounting examines the intent behind financial irregularities (Rezaee & Riley, 2010, p. 12). According to DiGabriele, forensic auditors must not only be financially astute but also interested in finding out why things happen, since many actions are beyond the reach of routine audits (DiGabriele, 2008, p. 333). The increasing use of forensic services across the globe can be attributed to a series of famous corporate scandals that have revealed limitations of the conventional audit paradigm, including Enron, WorldCom, and Lehman Brothers cases. After the scandals at Satyam and Punjab National Bank (PNB), forensic accounting has gained prominence in India. Consequently, standards for forensic auditing have been developed by ICAI and other organizations (ICAI, 2020, p. 8).

Regarding Fraud Models and Behavioral Theories, behavioral fraud models have played a vital role in the development of forensic accounting theory. There are three vital elements that lead to fraud: Pressure, Opportunity, and Rationalization. Cressey's (1953) Fraud Triangle framework demonstrates how a combination of personal justifications, inadequate internal controls, and financial strain can facilitate fraud. Critics, however, contend that the model oversimplifies the psychological profiles of fraud perpetrators (Cressey, 1953, p. 45).

Further, Wolfe and Hermanson (2004) have proposed the Fraud Diamond, enriching it with a fourth axis, capability, to incorporate the fraudster's expertise, assurance, and authority to take advantage of system vulnerabilities (Wolfe & Hermanson, 2004, p. 39). The fourth dimension is particularly applicable to Indian situations such as IL&FS or Yes Bank, where the senior management enjoyed singular access and control. Therefore, arrogance and competence are added as key drivers in Crowe Horwath's (2011) The Fraud Pentagon, further enhancing the list of fraud motivations. As demonstrated by the acts of Ramalinga Raju of Satyam and Rana Kapoor of Yes Bank, these factors explain why some people believe they are above accountability (Horwath, 2011, p. 15). Furthermore, Rezaee and Riley (2010) state that transition economies with underdeveloped regulatory frameworks, such as India, are at the highest risk of fraud (Wolfe & Hermanson, 2004). Therefore, in contrast to predictive or

preventive forensic tools, Indian case studies are primarily post-fraud-oriented, indicating a relevant research gap. Therefore, this study seeks to address this gap using evidence from Indian Case studies.

Regarding the limitations of traditional audit and governance, SEBI (2020) and the Ministry of Corporate Affairs (2019), among others, have reported persistent weaknesses in audit quality, internal controls, and Board supervision in Indian companies. Statutory audits often rely on data provided by management, which can weaken their ability to detect fraud (SFIO, 2021, p. 40). The RBI observed that fraudulent transactions remain undetected in banking and NBFCs due to overreliance on core banking software, a lack of forensic cross-verification, and the absence of independent transaction mapping (RBI, 2020, p. 17). The ICAI (2020) highlighted the necessity of incorporating forensic elements into statutory audits and professional practices.

Theoretical Framework

The study of the anatomy of corporate fraud requires not only awareness of financial malpractice but also an understanding of the factors that enable such practices. Over the years, various behavioural theories of fraud have helped explain why individuals indulge in fraudulent financial behaviour, especially within environments that lack proper internal control systems. The current study uses three existing theories of fraud, namely the Fraud Triangle, the Fraud Diamond, and the Fraud Pentagon, to examine India's most notorious cases of corporate fraud. **The Fraud Triangle Model** Developed by criminologist Donald Cressey in the 1950s, it remains one of the most widely used models in forensic analysis and auditing to date. The model states that there are three elements essential for committing any fraud, which include pressure, opportunity, and rationalisation (Cressey, 1953, p. 45). In the Indian cases analysed, including those of Satyam and DHFL, it was mostly financial or reputational pressure that acted as the impetus. This could be to satisfy market demand or to hide losses, among other reasons, with pressure as the cause. Vulnerabilities in internal controls and regulations gave the perpetrators the opportunity to manipulate accounting entries or evade the system. Finally, the rationalization stage involved excuses such as saving the business or simply 'borrowing for a short while', a state of mind well explained by the confessional letter in Satyam's case. From this perspective, forensic accounting is employed not only as a means of discovering fraud, but also predicting potential signs of trouble in relation to the three elements.

The Fraud Diamond Model Although the Fraud Triangle explains the 'why' behind fraud, it does not necessarily deal with the 'how'. This is where Wolfe and Hermanson (2004) came up with the concept of the Fraud Diamond, which is comprised of four components, including 'capability'. Capability can be defined as someone's status, intelligence, pride, and manipulation skills (Wolfe & Hermanson, 2004, p. 39). This principle would be especially relevant when there is a fraudulent situation where managers misuse their authority to circumvent any internal control mechanisms or dissenting opinions. For example, in the IL&FS case, a select group of insiders authorised circular lending across companies while auditors and other stakeholders remained clueless about the magnitude of fraud being committed. Similarly, Yes Bank's Rana Kapoor abused his position of authority to approve risky loans and hide NPAs. The focus on capabilities underlines the importance of additional, deeper forensic methods beyond normal

auditing, such as detection systems for insiders, access control auditing, and behaviour analysis of key executives.

The Fraud Pentagon Model. In addition to the existing elements of fraud risk factors, Crowe Horwath LLP (2011, p. 15) proposed the concept of the Fraud Pentagon, in which arrogance and competence also figure. Arrogance refers to a sense of invulnerability and is often exhibited by long-tenured CEOs or entrepreneurs who believe they can never be governed by any rule. On the other hand, competence is nothing but the ability to commit fraud with a high degree of technical skill. Both aspects are evident in several fraud incidents in India. Raju's control over the company's affairs and the creation of fictitious assets were examples of arrogance and incompetence.

A forensic perspective requires these dimensions to highlight the necessity of analytical tools not just to examine financial behavior but also psychological behavior and power plays within organizations. Forensic lifestyle audits, whistleblower examination, and data mining can be used as early warning devices when there is a failure to rein in arrogance or over competence.

Conceptual Integration: Forensic Accounting and Fraud Models

The integration of these three behavioral models through their application in the selected cases of fraud helps create a unified model for measuring fraud risk. Each of these components has an associated forensic measure that would reveal and prevent the fraud regardless of whether it was motivated by the pressure created by the Fraud Triangle or the arrogance created by the Fraud Pentagon. This method of analysis turns the field of forensic accounting into one that is proactive in nature.

The present study creates an integrated matrix that correlates particular behavioral factors with the related forensic measures to summarize the theoretical contributions of the Fraud Triangle, Fraud Diamond, and Fraud Pentagon. In this regard, it should be noted that the identification of fraud is not a single occurrence but rather a systemic process utilizing forensic techniques for all areas of fraud theory.

These relations are depicted in Figure 1 below, which highlights the application of theoretical knowledge into forensic techniques in complex corporate situations, such as in India.

Table 1: Behavioral Fraud Models and Forensic Response Matrix

Fraud Factor	Behavioural Indicator	Implications in Indian Cases	Forensic Accounting Tools & Techniques
Pressure ***(Fraud Triangle)***	• Aggressive financial targets • High debt or liquidity crunch	Satyam inflated profits, DHFL masked cash flow crisis	• Trend & ratio analysis • Cash flow tracking • Earnings manipulation detection

Opportunity ***(Fraud triangle)***	• Weak internal controls • Segregation of duties missing	PNB enabled SWIFT fraud bypassing CBS, IL&FS's unchecked related-party transactions	• Internal control evaluation • Transaction mapping • Control override detection tools
Rationalization ***(Fraud Triangle)***	• "It's Temporary" justification • Loyalty to the organization used to justify fraud	Satyam's founder claimed he was "protecting shareholders"	• Forensic interviews • Document narrative analysis • Email/ text audit trails
Capability ***(Fraud Diamond)***	• Access to critical systems • Technical manipulation skill	IL&FS insiders structured complex layered lending schemes	• Access rights audit • Insider behaviour analytics • Role-based monitoring systems
Arrogance ***(Fraud Pentagon)***	• Belief in being untouchable • Avoidance of scrutiny	Yes Bank's CEO bypassed internal checks with impunity	• Executive lifestyle audits • Anonymous whistleblower report tracing • Public statement cross-checks
Competence ***(Fraud Pentagon)***	• Creation of fake firms/ shells • Complex circular transactions	DHFL used 260+ shell firms to siphon Rs. 31,000 crores	• Shell company network mapping • Beneficial ownership analysis • Transaction link tracing

Source: Depicted by Authors

Methodology

The study investigates the nature of corporate frauds in India, and the role forensic accounting might play in either preventing or detecting them, employing qualitative and multi-case study methods. A purely quantitative investigation would not be appropriate due to the complexities involved in financial crimes, including organisational crime, psychology, regulatory failure, and professional knowledge. In this study, the concept of forensic accounting is used to study the two main foundations of fraud through case studies of five well-known corporate fraud cases: Yes Bank, Dewan Housing Finance Limited (DHFL), IL&FS, Punjab National Bank-Nirav Modi, and Satyam Computers.

The above five cases were selected based on certain considerations: firstly, they all had a significant impact on their reputation and economy, they were formally investigated by the concerned regulatory agencies such as SEBI, SFIO, or the Ministry of Corporate Affairs, they

came from diverse sectors such as IT, banking, NBFC, and infrastructure, and there was sufficient information regarding them in public domain, including forensic audit report, financial information, investigative journalism, and legal disclosure. This ensures that the relevance and richness of information are met in this study. The data collected for this study is secondary data extracted from credible sources of reports. Such reports included publicly available forensic audit reports, annual filings of companies, official reports by regulatory authorities, investigation reports by SEBI or SFIO, financial news sources, and relevant academic literature.

Each case was first analysed by building its narrative timeline, which included all key participants, decisions, and transactions involved in the fraud scheme. Then, the behavioural aspects of each fraud were analysed using three existing theories, namely the Fraud Triangle by Cressey (1953), Fraud Diamond by Wolfe and Hermanson (2004), and the Fraud Pentagon from Crowe Horwath (2011). Such an approach facilitated a structured analysis of the motives (such as pressure or rationalisation) as well as opportunities and capabilities involved in each fraud, such as arrogance or technical expertise. Then, this perspective was coupled with the evaluative analysis of forensic accounting procedures to establish the point of possible interventions. Finally, cross-case synthesis was performed to identify typical fraud patterns and governance flaws as well as forensically valuable triggers in such situations.

Furthermore, since this research is purely secondary data-based, it does not necessitate direct human interaction or primary data collection. Thus, no formal ethical clearance was needed. All sources are, however, quoted openly and respectfully. The purpose of the study is not to apportion blame to any specific individual or organisation, but rather to use these actual cases as educational tools to further improve the role of forensic accounting in fraud detection and prevention in emerging economies.

Case Analysis

Satyam Computer Services Ltd. (2009)

The Satyam scam of 2009 is one of the most surprising instances of corporate deceit in Indian history. The firm, formerly known as ‘India’s Enron’, acknowledged that it had inflated its profits and assets over several years before finally reporting a ₹7,000 crore discrepancy in its accounts. The scam was revealed when the founder, as well as erstwhile chairman, Ramalinga Raju, wrote a confession letter to the Board of Directors in which he acknowledged fudging accounts to show fictitious cash balances and exaggerated revenues (Securities and Exchange Board of India [SEBI], 2018, p. 4). From 2003 to 2008, Satyam repeatedly inflated its revenue and profit numbers to meet market expectations. Investigations showed that around 7,561 fake invoices were generated using another server system (My Home Hub) outside the firm’s SAP ERP platform (Serious Fraud Investigation Office [SFIO], 2010, p. 91). In addition, 356 fictitious companies were used to make sham salary payments and reimbursements to employees, adding more layers of deceit (PricewaterhouseCoopers [PwC], 2009, p. 17).

Under the Fraud Triangle approach, all the elements can be seen. Firstly, there was pressure in the shape of high levels of expectations set by the company’s stockholders and the markets.

According to Raju, his actions started with the aim of filling the gap between what was expected of him and actual performance, but later on, he found himself in a vicious circle (Cressey, 1953, p. 47). Mis-opportunity was created because of a lack of segregation of duties, poor controls over the audit committee's work, and excessive powers given to the promoter of the firm (Raju, 2009, as quoted by SFIO, 2010, p. 43).

The fraud Pentagon approach digs deeper into the behavioural analysis. Arrogance was clearly displayed by Raju since he controlled the corporate structures and even the Board of Directors, which included individuals who were family members or close associates of Raju. The competence aspect is also valid in this case since manipulation at such a level was necessary to alter the bank statements, produce false invoices, and build hidden infrastructure (Crowe Horwath LLP, 2011, p. 15).

From a forensic accounting standpoint, there were some missed chances in the Satyam scandal that should have served as an early warning. Forensic examination of the pattern of cash flow would have shown discrepancies between the bank balance and the earnings statement. Forensic metadata and forensic email examination would have shown manipulation of communication channels for approving invoices. Employee data analytics would have identified discrepancies in the payroll of fake employees. Furthermore, behavioural risk assessment of the executive management, which is a part of modern forensic accounting, would have identified Raju's overreaching and untouchable authority as risks (Rezaee & Riley, 2010, p. 62).

The forensic audit conducted after the scandal by Deloitte and Luthra & Luthra revealed numerous inconsistencies, including falsified interest income and non-reconciliation of TDS (tax deducted at source) entries. All these signs were forensically apparent had independent validation been practised (SFIO, 2010, p. 125). The Satyam scandal resulted in increased regulatory changes in India, such as the creation of NFRA and the amendment of the Companies Act, 2013. It will be remembered forever for highlighting how much can go wrong if a normal audit is unable to work, and no use is made of forensic procedures in financial matters.

Punjab National Bank – Nirav Modi Fraud (2018)

The 2018 Punjab National Bank (PNB) fraud involving diamond jeweller Nirav Modi and his group is regarded as the largest bank fraud in Indian history, amounting to about ₹13,000 crore (USD 2 billion). This fraud revealed many basic deficiencies in banking in the public sector, which included the misuse of certain documents, such as Letters of Undertaking (LoUs). The fraud had been carried out for a period of at least seven years by two young PNB employees at the Brady House branch of the bank in Mumbai, where the issuance of LoUs was not even recorded in CBS (Central Vigilance Commission, 2018, p. 13).

The LoUs were created fraudulently through SWIFT (Society for Worldwide Interbank Financial Telecommunication) messages that were not part of the CBS system. This loophole helped the accused obtain foreign credits by providing false guarantees in relation to other banks in India. The companies of Nirav Modi would take advantage of such credits on an indefinite basis, thus creating a vicious cycle of credit. The abuse was found out only because

one of his companies requested a new LoU, which the concerned authority rejected without providing any margin (Reserve Bank of India, 2018, p. 7).

As per the Fraud Triangle theory, the pressure to live an international luxurious lifestyle and to run a luxurious jewellery business empire across various countries was the critical reason behind this fraud. In addition to that, an opportunity presented itself because there were weaknesses in the processes, such as failure to integrate the SWIFT-CBS system, and no four-eyes control (maker-checker concept). The rationalisation part may have been justified by Nirav Modi's constant remark, "It was a business strategy." (Cressey, 1953, p. 48).

As far as the Fraud Diamond is concerned, capability played an important role in the crime. Nirav Modi, along with his accomplices, understood the vulnerabilities of the banking system and systematically exploited these loopholes. The role of the complicit insider with knowledge of SWIFT also played an important part (Wolfe & Hermanson, 2004, p. 40). There was also substantial planning that took place when forming several shell companies that were used for the purpose of transferring credit among themselves (SFIO, 2019, p. 21).

Fraud Pentagon helps crack down on behavioural factors. Arrogance can be identified through the size of the scheme and its arrogance in the launch of luxury products at the World Economic Forum despite growing debts. Competence was demonstrated in terms of borderless shell structures, related party structures, and mysterious accounting (Crowe Horwath LLP, 2011, p. 15).

If there had been controls involving forensic accounting at the compliance and operational levels, an alert could have been generated. For example, the transaction profiling technique could have revealed frequent LoUs to the same party without any proper collateral. The forensic IT audit procedure could have alerted to the dangerous separation between SWIFT and CBS systems. Frequent due diligence on vendors would have shown the high connectivity between companies owned by Modi, taking loans from different banks through the same LoUs basis. Reports post-fraud investigation by the RBI and SFIO revealed that even basic forensic alerts like frequent transactions to the same pool of foreign counterparties, backdating of Letters of Understanding (LoUs), and no board approval of limit were ignored due to failures in audit procedures (RBI, 2018, p. 12; SFIO, 2019, p. 25).

This led to regulations requiring full integration between SWIFT and CBS, stricter LoU procedures, and enhanced forensic analysis in auditing banks. Nonetheless, it is a landmark case where the adoption of preventative forensic accounting techniques would have helped to limit or avoid such fraudulent activities.

IL&FS Collapse (2018)

The IL&FS default in 2018 exposed governance weaknesses that had been lurking beneath the surface in India's shadow banking system. IL&FS, which was a highly-rated NBFC with asset size exceeding ₹91,000 crore, defaulted on its debt amounting to over ₹94,000 crore, triggering fear across the entire financial ecosystem (Ministry of Corporate Affairs [MCA], 2019, p. 9). However, unlike the pure embezzlement cases, the IL&FS default was driven by accounting

manipulation, careless lending of projects with inadequate due diligence, and concealing bad debts. Through a complex network of over 340 subsidiaries and special purpose vehicles (SPVs), some of which were loss-making, the company attempted to mask the real financial condition of the organisation (Grant Thornton, 2019, p. 4). It was revealed through forensic auditing that the SPVs borrowed money from each other without any internal authorisation or proper risk assessment.

Fraud triangle theory suggests that pressure to show strength and maintain AAA ratings forced management to conceal poorly performing assets and fund unsuccessful ventures through internal lending facilities. Opportunities were provided by a lack of adequate oversight from the board of directors, an ineffective risk committee, and poor audit functions. The rationalisation factor was embedded in the group's need to maintain liquidity in the infrastructure sector, which is normally regarded as too important to fail (Cressey, 1953, p. 49). Fraud diamond can be very useful here. The managers, especially those from the finance department, exhibited great competence. The managers designed a system of revolving credit where new credit facilities would be used to repay the old ones within the company's affiliated units to avoid default in the records. Such financial engineering would require access to the internal accounting details of the company and its limitations in the auditing process (Wolfe & Hermanson, 2004, p. 40). In addition, weaknesses in internal controls meant that the audit committee would get inputs from management alone.

The Fraud Pentagon also offers explanations for the behavioral patterns. There was arrogance in the disregard by senior management for early warning signs by credit analysts and ratings agencies. Even though there was pressure to be liquid, there was continued issuance of new debt because of the exaggerated sense of control over systemic risks. Their expertise in using special purpose vehicles (SPVs) and off-balance sheet structures was indeed technical, but it served to hide more than uncover (Crowe Horwath LLP, 2011, p. 15).

From the point of view of forensic accounting, there are some apparent intervention points in the IL&FS case study. For instance, a network analysis of fund transfers between companies within the corporate group would have shown that the pattern of loan transactions was uncharacteristically high among the loss-making companies. The solvency test on cash flows, as opposed to the profit-and-loss test, would have shown that the company had been borrowing beyond its capacity. Lastly, forensic analysis of board meetings and approvals would have shown that risks were being ignored or even manufactured.

The incident led to the rethinking of regulations regarding NBFCs. The RBI introduced tighter rules about liquidity coverage ratios, while the SEBI made the disclosure of related party transactions compulsory. However, the IL&FS episode can be cited as one in which the use of forensics would have prevented a contagion from spreading through banks and mutual funds.

DHFL Fraud (2019)

The scandal of DHFL in 2019 revealed one of India's biggest and most technologically sophisticated cases of financial fraud, with damages amounting to over ₹31,000 crore. Being a large non-banking financial company, DHFL was once a major stakeholder in the housing

finance sector of India. However, according to the forensic audit done by KPMG and subsequent investigations by the ED and SFIO, DHFL siphoned off public funds using more than 260 shell companies, the majority of which had dummy directors and employees (KPMG, 2020, p. 22; SFIO, 2021, p. 13). According to the forensic audit, DHFL extended numerous crores of rupees to dummy or associated entities that failed to pay back the debt. The money was marked as a regular asset on the company's balance sheet, but the payments had already been funnelled out via shell firms or evergreened so that the default would not be recorded. On some occasions, the supporting documentation for the transactions had not even existed or was fabricated (SFIO, 2021, p. 28).

The fraud triangle pressures, on the other hand, resulted from excessively ambitious business growth aspirations and the need to safeguard perceptions about the firm from investors as well as rating agencies. This is because in the period between 2014 and 2018, DHFL issued NCDs and bonds to the tune of thousands of crores, thereby exerting pressure on liquidity and creditworthiness. The opportunity in this scenario arose from inadequate supervision by the regulator, which was the case for the NBFCs that had lesser supervisory oversight compared to the commercial banks (Cressey, 1953, p. 50).

Under the Fraud Diamond, capability was ingrained in the organizational leadership. The promoters, Kapil and Dheeraj Wadhawan, possessed both technical and administrative expertise required for diverting huge sums of money through their controlled organizations. They bypassed internal procedures, distorted the rating process, and coerced the officials of public sector banks to provide concessional financing (Wolfe & Hermanson, 2004, p. 41).

Further behavioural insights come from The Fraud Pentagon. Promoters' arrogance is manifest in their lavish lifestyles, private jets, overseas luxury properties, and ties to influential political and business figures, despite the growing liquidity problems at the company. Demonstrations of competence include the use of layering, documentation, and identity control techniques. The shell corporations created in this fraud scheme are so well-designed that they pass elementary due diligence efforts by third-party audit firms and rating agencies for years (Crowe Horwath LLP, 2011, p. 15).

From the forensic accounting point of view, there were different warning signs that were overlooked. The forensic KYC audit of the borrowers would have identified fake companies and repetitive identification numbers. Cluster analysis of the loan portfolio would have identified that a significant number of valuable loans were given to individuals who had similar addresses, directors, or phone numbers. Forensic investigation of internal emails would have helped to understand the mechanism to dodge credit checks (KPMG, 2020, p. 32).

Following the detection of fraud, DHFL was initiated into insolvency proceedings under the Insolvency and Bankruptcy Code (IBC), resulting in the takeover of its assets by the Piramal Group via the resolution process. In this context, the case saw a change in RBI regulations regarding the management of NBFCs and marked its first use of the IBC.

Yes Bank Governance Crisis (2020)

The Yes Bank crisis came to light in early 2020 when the RBI took charge of the bank's management and imposed a restriction on withdrawals following the revelation that the bank had been imprudently inflating its asset book and understating non-performing assets (NPAs). This crisis, valued at ₹24,000 crore in terms of stressed loans, arose due to the pattern of indiscriminate lending, conflict of interest, and accounting misrepresentation facilitated by poor governance practices under CEO Rana Kapoor (RBI, 2020, p. 11; SEBI, 2020, p. 17).

EY forensic audits revealed that Yes Bank had been making tremendous loans from 2016 to 2019 to companies suffering financial hardships and were heavily leveraged like IL&FS, DHFL, Reliance ADA, Cox & Kings, and Radius Developers, most of whom had failed or were on the verge of failing. The company claims that these huge loans were made in exchange for favors and kickbacks as companies with interests of the family owned by Rana Kapoor had investments in borrowing companies (Ernst & Young, 2020, p. 26).

In terms of pressure, according to the Fraud Triangle, the same is driven by an aggressive target setting by the CEO and an objective of making Yes Bank a competitor for HDFC and ICICI. This pressure on rapid increase of the loan book came from top management and had internal pressure on employees to disburse quotas. Opportunities could be found in the top-down decision making style of Kapoor as well as poor Board governance with critical Risk Management and Audit Committees being controlled by the CEO's office.

According to the Fraud Diamond model, the driving factor identified is capability. Kapoor had the capability to access the internal system freely and it was found that he had the ability to bypass any second-level review process. Kapoor built personal relationships with some groups of borrowers, resulting in an excessive lending. Lending was done in stages, either through non-convertible debentures or through alternative investment funds (Wolfe & Hermanson, 2004, p. 43).

Arrogance was evident among members of the Fraud Pentagon, with Kapoor showing this through statements made publicly and his lavish living arrangements, including paintings he collected, his homes, and hobnobbing with A-list celebrities. Competence was another characteristic seen in the sophisticated structure of credit deals and off-balance sheet operations which created an impressive financial picture compared to the real one (Crowe Horwath LLP, 2011, p. 15).

Several forensic accounting techniques could have helped prevent this problem much earlier. For instance, related party transactions could have been audited to detect any unusual relationships between the borrowing companies and those owned by members of the Kapoor family. Risk behavior analysis could have detected centralization of credit decisions and overrides by internal credit committees. Cash flow monitoring and credit layering analysis could have exposed the actual financial standing of the key borrowers of Yes Bank, who all had telltale signs of trouble.

After the crisis, the RBI required new governance standards to be set for private banks, splitting up the CEO and MD positions, and limiting the tenure of promoter CEOs. The bank was saved by a restructuring process spearheaded by the State Bank of India, but this incident serves as an important lesson on the dangers of unfettered authority and lack of forensic auditing.

Discussion and Cross-Case Insights

From the above five famous financial scandals- Satyam Computers, PNB-Nirav Modi, IL&FS, DHFL, and Yes Bank-, it is clear to see certain recurring themes of organizational behavior, human intentions, and lack of forensics among others that highlight the emergence and process behind corporate financial frauds. Also, this is explainable under the social context such as the key involvement is from so-called elite part of soceity who have higher status and still their intention to deviate just for their own interest (Reurink, 2016, p.391and Green, 2004, p.6) and financial achievements. Despite operating in diverse industries, there is a common nexus of human intentions, governance failures, and lack of forensic scrutiny across the board.

The first common trend from the above mentioned examples was the Fraud Triangle of pressure, opportunity, and justification. In each situation, managers faced immense pressure to grow, satisfy stakeholders or maintain good ratings. The existence of pressure along with poor governance frameworks such as inadequate audit processes (as in the case of PNB) and lack of board activity (as in the case of IL&FS), created favorable conditions for fraud. It is clear that in each of the above cases, the culprits justified their actions as necessary means to an end (Cressey, 1953, p. 55).

The Fraud Diamond and Pentagon frameworks build upon this knowledge by highlighting arrogance, and expertise. In all these cases, people behind the frauds were technically knowledgeable and possessed significant organizational power. Therefore, Raju's dual control over the information technology systems and finances of Satyam, Wadhawans' knowledge of the gaps in regulations concerning NBFCs, and Rana Kapoor's approval rights over loans at Yes Bank exemplify the role that capability, arrogance, and competence played in sustaining the fraud (Wolfe & Hermanson, 2004, p. 43; Crowe Horwath LLP, 2011, p. 15). Arrogance and confidence enabled these key people to ignore ethical boundaries, leading to an eventual downfall.

A constant observation from cross-case analysis is the lack of contemporary forensic oversight in these organizations. Traditional audits based on compliance could not catch irregularities early. An early alert system involving the use of digital footprint tracking, pattern-based behavior analysis, related party detection, and leveraging data analytics would have identified potential concerns early on. Satyam and DHFL cases clearly show the importance of forensic tools such as fund flows analysis and employee access data analysis in preventing any financial frauds.

Furthermore, the scandals suggest that there is a need for structural embedding of forensic accounting into regulatory frameworks and organizational systems, rather than being an ad hoc solution to a problem that emerges. There have been attempts by both the RBI and the SEBI to

integrate forensic audits in their supervision processes, but what is needed is forensic vigilance, moving from forensic investigation after fraud to forensic prevention of fraud before it occurs.

Proposed Forensic Accounting Framework for Emerging Economies

From the perspective gained through behavioral fraud theories as well as analysis of various corporate fraud cases that occurred in India, this research proposes an Integrated Behavioral-Forensic Risk Framework (IBFRF) for emerging economies. The main goal of this framework is to convert forensic accounting practices from a reactive practice into a proactive fraud risk management system. The IBFRF combines behavioral risks associated with fraud with forensic tools, information technology, and regulatory mechanisms to ensure the early detection and prevention of fraud.

This framework has been designed in form of a hierarchical model consisting of five different layers: (i) behavioral risk identification, (ii) red flag identification, (iii) forensic tools identification, (iv) continuous monitoring, and (v) governance and regulation. These five layers correspond to different theoretical concepts based on fraud triangle, fraud diamond, and fraud pentagon, together with forensic interventions that were found to be missing in the analyzed cases.

The first layer, Behavioural Risk Identification, focuses on recognising the underlying drivers of fraudulent behaviour within organisations. Drawing from Cressey (1953), Wolfe and Hermanson (2004), and Crowe Horwath (2011), this stage identifies six core risk dimensions: pressure, opportunity, rationalisation, capability, arrogance, and competence. These behavioural indicators are not merely abstract constructs but are observable through organisational patterns such as aggressive financial targets, excessive managerial dominance, weak internal controls, and over-centralisation of authority. For instance, the pressure to maintain market expectations was evident in the Satyam case, while opportunity arising from Loopholes in systems were an important factor behind the PNB scam. Through behavioural risk assessment institutionalization, organizations would be able to spot these weaknesses even before they turn into financial malpractices.

The second step, Red Flag Mapping, involves translating these behavioural risks into tangible warning signs. This process is very important in making the connection between theory and practice. The different behavioural risks are linked to financial and operational irregularities. These include unexpected growth of revenues without cash flow, recurring high-value financial transactions with same counterparties, frequent transactions through shell companies, and unusual transactions with related parties. Circular financing at IL&FS was an illustration of this process, while the DHFL case showed clustering of loans from connected organizations.

Thirdly, the layer Forensic Tools Integration correlates each red flag with an appropriate forensic accounting tool. Unlike audit procedures that use sampling and compliance checks in large numbers, forensic tools involve a more investigative process using data-based tools. Tools such as ratio and trend analysis, transaction mapping, network/link analysis, IT forensic audit, and behaviour analytics can be used to detect manipulative patterns within the system. In

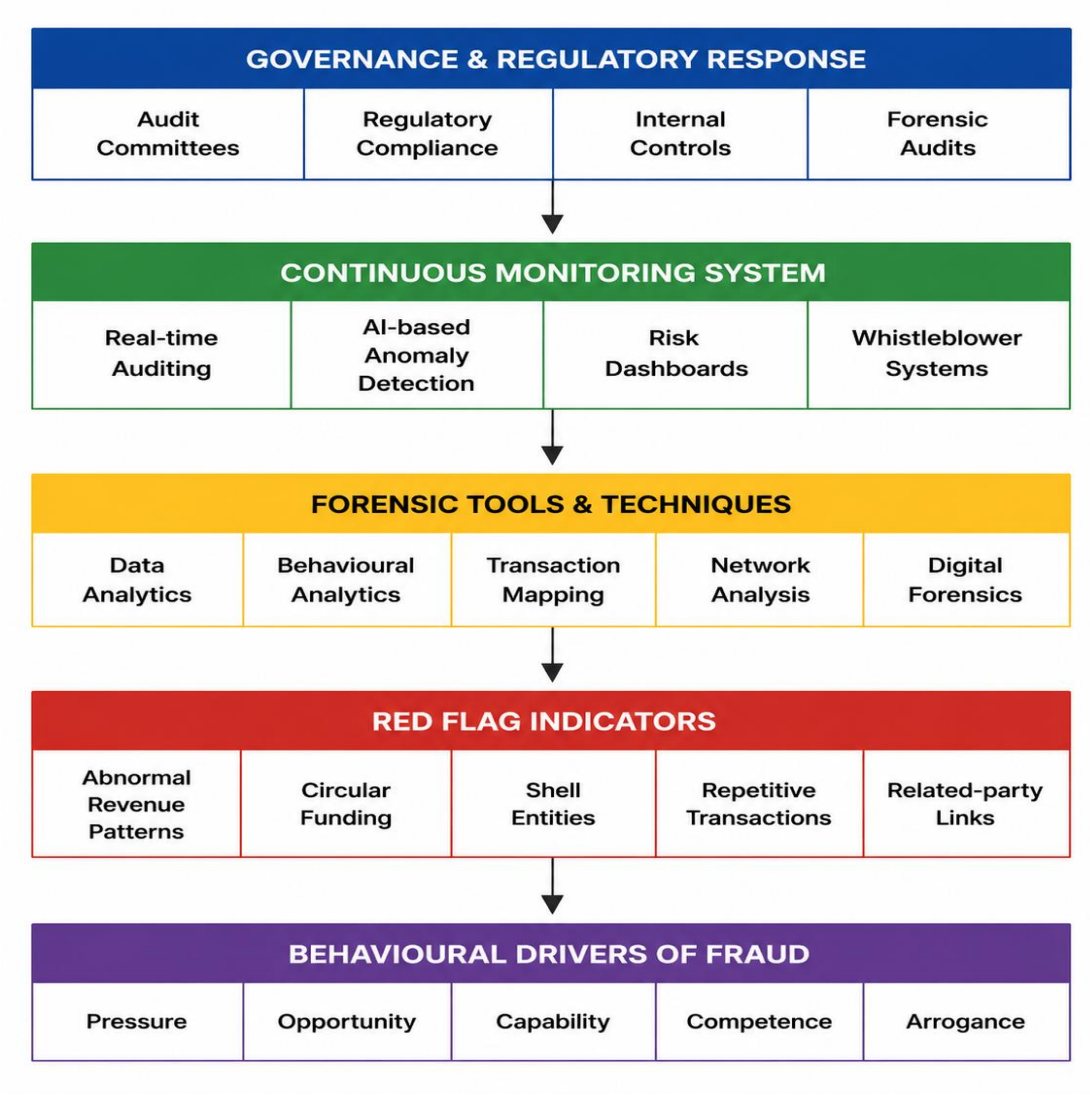
DHFL, network analysis would reveal the links between the shell companies, whereas an IT forensic audit would detect the issue between SWIFT and CBS systems in PNB fraud cases. Additionally, behavior analytics and email tracing would identify the risk of executive overrides in the Yes Bank case.

The fourth component, Continuous Monitoring and Real-Time Surveillance, is a radical change from the concept of periodic auditing to continuous forensic monitoring. Consistently, one of the major flaws identified during all case studies was the lack of a system that could provide real-time surveillance. As recommended by the new framework, technology should be incorporated into audit procedures. Some of these technologies may include the use of advanced technology such as artificial intelligence, machine learning, and other techniques to continuously monitor the transaction activities. Forensic intelligence through continuous auditing will allow companies to detect any anomalies during the process and alert the concerned parties about any problems.

The fifth and last layer of forensic governance, which is called Governance and Regulatory Integration, seeks to make sure that the information that has been gained from the forensic process results in effective control and intervention measures. This layer focuses on the contribution that boards of directors, audit committees, and regulators can play in making forensic auditing part of their organization. Corporations should conduct forensic audits periodically in high risk zones, improve their internal control systems, and guarantee audit committee independence. Regulators such as RBI and SEBI can add more value to governance by using forensic auditing in supervision and disclosure of high risk deals.

As a closed-loop process, feedback from each stage is incorporated into risk identification, allowing the process to improve continuously. Behavioral theories are used to detect red flags, which are then used for conducting forensic investigations, resulting in constant monitoring and governance. The approach adopted by the IBFRF allows organizations to view the prevention of fraud as a continuous process rather than an event. In summary, the IBFRF seeks to reorient the field of forensic accounting by positioning it as a governance tool rather than a crisis management tool. By combining behavioural theories, technology, and regulation, the framework offers a robust solution to the challenges posed by corporate fraud in emerging markets.

Figure 1: Closed-loop system enabling proactive fraud risk detection and prevention



Source: **Depicted by the authors**

The framework illustrates the transition from behavioural risk identification to continuous forensic monitoring and governance response, forming a closed-loop fraud prevention system.

Conclusion and Policy Recommendations

The analysis of the five largest corporate scandals in India, for instance, Satyam, PNB-Nirav Modi, IL&FS, DHFL, and Yes Bank, indicates that despite the variation in the sector and scale, all corporate scandals have one thing in common—they result from a mix of motivational, structural, and governance issues. In each case, top-down pressure, uncontrollable opportunities, and rationalised malfeasance have been enough to bring down even the largest corporations. However, the distinguishing factor among these scandals is neither the

complexity of the fraud nor the lack of detailed accounting procedures. The only thing missing in these cases was forensic accounting intervention at an earlier stage.

The findings show the importance of embedding forensic accounting practices as an active monitoring mechanism rather than a crisis response. Incorporation of forensic data analytics, risk profiling, and digital transaction monitoring in financial monitoring processes can make fraud detection proactive in nature. The regulators, such as RBI, SEBI, and MCA of India, must coordinate in developing a comprehensive forensic compliance system, which incorporates the elements of corporate governance with fraud analysis. Further, there must be an Senhancement in the forensic acumen of auditors, compliance professionals, and directors through mandatory professional courses and certifications. These cases also show the personal interest, status, and opportunity under the notion of deviance that has emerged as larger and stronger social deviance narratives in society.

More broadly, the paper reaffirms that forensic accounting is not a technical science but a governance strategy. If employed effectively, it can help restore trust in financial institutions, curb opportunism, and protect the people's wealth from any risk of abuse. Indeed, India's governance initiatives have made such integration possible, but what matters now is continued commitment, technological support, and ethical governance to learn from the lessons of those sensational scandals.

References

Central Vigilance Commission. (2018). *Report on Systemic Lapses in Punjab National Bank – LoU Fraud* (p. 13). New Delhi: Government of India.

Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement* (p. 45). Montclair, NJ: Patterson Smith.

Crowe Horwath LLP. (2011). *The Fraud Pentagon: Addressing the Five Key Factors of Fraud Risk* (p. 15). Chicago, IL: Crowe Horwath LLP.

Crumbley, D. L., Heitger, L. E., & Smith, G. S. (2015). *Forensic and Investigative Accounting* (7th ed., pp. 19–21). Chicago, IL: CCH Incorporated.

DiGabriele, J. A. (2008). An empirical investigation of the relevant skills of forensic accountants. *Journal of Education for Business*, 83(6), 331–338. https://doi.org/10.3200/JOEB.83.6.331-338

Ernst & Young. (2020). *Forensic Audit Report on Yes Bank Lending Practices* (p. 26). Mumbai: EY India.

Grant Thornton. (2019). *Forensic Audit Report of IL&FS Group Entities* (pp. 4, 23). Mumbai: Grant Thornton India LLP.

Green, S. P. (2004). The concept of white collar crime in law and legal theory. *Buffalo Criminal Law Review*, *8*(1), 1-34.

Huber, W. D. (2013). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research*, 9(2), 28–48.

ICAI. (2020). *Forensic Accounting and Investigation Standards: Exposure Draft* (p. 8). New Delhi: The Institute of Chartered Accountants of India.

KPMG. (2020). *Forensic Audit Report on DHFL* (pp. 22, 32). Mumbai: KPMG India.

Ministry of Corporate Affairs. (2019). *Report of Committee on Corporate Governance Framework in India* (p. 13). New Delhi: Government of India.

Ministry of Corporate Affairs. (2019). *Report on the Governance Failures in IL&FS Group* (p. 9). New Delhi: Government of India.

Ozkul, F. U., & Pamukcu, A. (2012). Fraud detection and forensic accounting. *International Journal of Business and Social Science*, 3(19), 65–70.

PricewaterhouseCoopers. (2009). *PwC Internal Memo on Satyam Investigation* (p. 17). Hyderabad: PwC India.

Rajasekar, D., & Manoharan, P. K. (2019). Auditors' failure in the Satyam scam: A study on post-mortem audit accountability. *Journal of Forensic Accounting Research*, 1(2), 1–18. https://doi.org/10.2308/jfar-52694.

RBI. (2020). *Financial Stability Report, June 2020* (p. 17). Mumbai: Reserve Bank of India.

Reserve Bank of India. (2018). *Supervisory Assessment of Punjab National Bank – Fraudulent LoUs Case* (pp. 7, 12). Mumbai: Department of Banking Supervision.

Reserve Bank of India. (2020). *Governance Assessment Report: Yes Bank Ltd.* (p. 11). Mumbai: Department of Supervision, RBI.

Reurink, A. (2016). "White-Collar Crime": The concept and its potential for the analysis of financial crime. *European Journal of Sociology/Archives Européennes de Sociologie*, *57*(3), 385-415.

Rezaee, Z., & Riley, R. (2010). *Financial Statement Fraud: Prevention and Detection* (p. 28). Hoboken, NJ: John Wiley & Sons.

SEBI. (2018). *Order against Ramalinga Raju and others in the matter of Satyam Computer Services Ltd.* (p. 4). Mumbai: Securities and Exchange Board of India.

SEBI. (2020). *Annual Report 2019–2020* (p. 22). Mumbai: Securities and Exchange Board of India.

SEBI. (2020). *Enforcement Report on Yes Bank Ltd.* (p. 17). New Delhi: Securities and Exchange Board of India.

SFIO. (2010). *Report on Investigation into the Affairs of Satyam Computer Services Ltd.* (pp. 43, 91, 125). New Delhi: Ministry of Corporate Affairs, Government of India.

SFIO. (2019). *Investigation Report on Nirav Modi–PNB Case* (pp. 21–25). New Delhi: Ministry of Corporate Affairs, Government of India.SFIO. (2021). *Investigation Report on Dewan Housing Finance Corporation Ltd.* (pp. 13, 28). New Delhi: Ministry of Corporate Affairs, Government of India.

SFIO. (2021). *Investigation Report: IL&FS Group Case* (p. 40). New Delhi: Serious Fraud Investigation Office, Government of India.

Sutherland Edwin H.(1983). White Collar Crime: The Uncut Version (New Haven, Yale University Press).

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *CPA Journal*, 74(12), 38–42.